Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

О.А. Пихтилькова, А.Н. Благовисная

СРАВНЕНИЯ И СИСТЕМЫ СРАВНЕНИЙ

Методические указания

Рекомендовано к изданию редакционно-издательским советом федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» для обучающихся по образовательной программе высшего образования по направлению подготовки 02.03.01 Математика и компьютерные науки

Оренбург
2018

УДК 511.2 (076.5)
ББК 22.132. я7
П 35

Рецензент – доцент, кандидат физико-математических наук Т.М. Отрыванкина

Пихтилькова, О.А.
П 35 Сравнения и системы сравнений: методические указания / О.А. Пихтилькова, А.Н. Благовисная; Оренбургский гос. ун-т – Оренбург: ОГУ, 2018. – 48 с.

Методические указания предназначены для выполнения расчетно-графического задания по разделу дисциплины «Теоретико-числовые методы в криптографии».

Методические указания включают примеры решений типовых задач и задания для самостоятельного выполнения. Методические указания составлены в соответствии с рабочей программой дисциплины «Теоретико-числовые методы в криптографии» для студентов направления подготовки 02.03.01 Математика и компьютерные науки.

УДК 511.2 (076.5)
ББК 22.132. я7

Содержание

Введение

Методические указания предназначены для студентов, обучающихся по направлению подготовки 02.03.01 Математика и компьютерные науки.

В методических указаниях приводятся 20 вариантов заданий для самостоятельного выполнения и пример решения и оформления одного варианта заданий.

Особенностью данных учебно-методических указаний является наличие в них прикладных задач криптографического содержания.

Содержание методических указаний соответствует рабочей программе дисциплины «Теоретико-числовые методы в криптографии» для студентов очной формы обучения направления подготовки 02.03.01 Математика и компьютерные науки.

1 Варианты заданий

Задание 1. Решить сравнения.

1.1. а) $4529x \equiv 328 (\mathrm{mod}\, 929)$; б) $1335x \equiv 385 (\mathrm{mod}\, 5595)$;

в) $1260x \equiv 406 (\mathrm{mod}\, 8218)$.

1.2. а) $3280x \equiv 297 (\mathrm{mod}\, 887)$; б) $1036x \equiv 287 (\mathrm{mod}\, 8218)$;

в) $1072x \equiv 896 (\mathrm{mod}\, 7184)$.

1.3. а) $4639x \equiv 425 (\mathrm{mod}\, 911)$; б) $1552x \equiv 152 (\mathrm{mod}\, 7184)$;

в) $1620x \equiv 324 (\mathrm{mod}\, 4068)$.

1.4. а) $3021x \equiv 501 (\mathrm{mod}\, 941)$; б) $1212x \equiv 510 (\mathrm{mod}\, 6924)$;

в) $1400x \equiv 315 (\mathrm{mod}\, 7385)$.

1.5. а) $4591x \equiv 203 (\mathrm{mod}\, 983)$; б) $1914x \equiv 418 (\mathrm{mod}\, 9482)$;

в) $2268x \equiv 162 (\mathrm{mod}\, 7641)$.

1.6. а) $6001x \equiv 398 (\mathrm{mod}\, 977)$; б) $1602x \equiv 266 (\mathrm{mod}\, 7974)$;

в) $1632x \equiv 170 (\mathrm{mod}\, 7718)$.

1.7. а) $4254x \equiv 681 (\mathrm{mod}\, 839)$; б) $1144x \equiv 462 (\mathrm{mod}\, 6008)$;

в) $2450x \equiv 225 (\mathrm{mod}\, 7825)$.

1.8. а) $5618x \equiv 335 (\mathrm{mod}\, 953)$; б) $1062x \equiv 399 (\mathrm{mod}\, 4491)$;

в) $2088x \equiv 192 (\mathrm{mod}\, 6924)$.

1.9. а) $3028x \equiv 528 (\mathrm{mod}\, 883)$; б) $1924x \equiv 143 (\mathrm{mod}\, 7202)$;

в) $1539x \equiv 216 (\mathrm{mod}\, 4491)$.

1.10. а) $4112x \equiv 365 (\mathrm{mod}\, 937)$; б) $1234x \equiv 385 (\mathrm{mod}\, 8043)$;

в) $1296x \equiv 448 (\mathrm{mod}\, 6008)$.

1.11. а) $324x \equiv 1628 (\mathrm{mod}\, 991)$; б) $2380x \equiv 445 (\mathrm{mod}\, 8380)$;

в) $1008x \equiv 162 (\mathrm{mod}\, 7974)$.

1.12. а) $628x \equiv 2006 (\mathrm{mod}\, 907)$; б) $1428x \equiv 707 (\mathrm{mod}\, 6524)$;

в) $1806x \equiv 126 (\mathrm{mod}\, 8043)$.

1.13. а) $625x \equiv 3214 (\mathrm{mod}\, 967)$; б) $2592x \equiv 276 (\mathrm{mod}\, 7944)$;

в) $2820x \equiv 340 (\mathrm{mod}\, 8380)$.

1.14. а) $407x \equiv 1350 (\mathrm{mod}\, 947)$; б) $1539x \equiv 627 (\mathrm{mod}\, 7641)$;

в) $1036x \equiv 532 (\mathrm{mod}\, 6524)$.

1.15. а) $509x \equiv 2627 (\mathrm{mod}\, 971)$; б) $1700x \equiv 665 (\mathrm{mod}\, 7825)$;

в) $3168x \equiv 198 (\mathrm{mod}\, 9482)$.

1.16. а) $425x \equiv 2966 (\mathrm{mod}\, 829)$; б) $2592x \equiv 304 (\mathrm{mod}\, 8992)$;

в) $1768x \equiv 234 (\mathrm{mod}\, 7202)$.

1.17. а) $349x \equiv 3508 (\mathrm{mod}\, 859)$; б) $2277x \equiv 605 (\mathrm{mod}\, 7953)$;

в) $1992x \equiv 216 (\mathrm{mod}\, 7944)$.

1.18. а) $401x \equiv 1328 (\mathrm{mod}\, 919)$; б) $1530x \equiv 255 (\mathrm{mod}\, 7718)$;

в) $2772x \equiv 264 (\mathrm{mod}\, 7953)$.

1.19. а) $529x \equiv 3452 (\mathrm{mod}\, 863)$; б) $1015x \equiv 203 (\mathrm{mod}\, 7385)$;

в) $2496x \equiv 224 (\mathrm{mod}\, 8992)$.

1.20. а) $452x \equiv 2911 (\mathrm{mod}\, 809)$; б) $1296x \equiv 510 (\mathrm{mod}\, 4068)$;

в) $2700x \equiv 435 (\mathrm{mod}\, 5595)$.

Задание 2. Решить системы линейных сравнений, используя греко-китайскую теорему об остатках.

2.1. а) $\begin{cases} x \equiv 7 (\mathrm{mod}\, 11), \\ x \equiv 3 (\mathrm{mod}\, 13), \\ x \equiv 6 (\mathrm{mod}\, 17), \\ x \equiv 1 (\mathrm{mod}\, 20). \end{cases}$ б) $\begin{cases} x \equiv 13 (\mathrm{mod}\, 15), \\ x \equiv 16 (\mathrm{mod}\, 17), \\ x \equiv 4 (\mathrm{mod}\, 19), \\ x \equiv 5 (\mathrm{mod}\, 12). \end{cases}$

2.2. а) $\begin{cases} x \equiv 14 (\mathrm{mod}\, 17), \\ x \equiv 5 (\mathrm{mod}\, 18), \\ x \equiv 2 (\mathrm{mod}\, 19), \\ x \equiv 1 (\mathrm{mod}\, 23). \end{cases}$ б) $\begin{cases} x \equiv 5 (\mathrm{mod}\, 27), \\ x \equiv 4 (\mathrm{mod}\, 29), \\ x \equiv 15 (\mathrm{mod}\, 19), \\ x \equiv 7 (\mathrm{mod}\, 15). \end{cases}$

2.3. а) $\begin{cases} x \equiv 9 (\mathrm{mod} 13), \\ x \equiv 5 (\mathrm{mod} 14), \\ x \equiv 7 (\mathrm{mod} 19), \\ x \equiv 11 (\mathrm{mod}\, 23). \end{cases}$ б) $\begin{cases} x \equiv 2 (\mathrm{mod}\, 23), \\ x \equiv 17 (\mathrm{mod}\, 21), \\ x \equiv 4 (\mathrm{mod} 13), \\ x \equiv 2 (\mathrm{mod} 15). \end{cases}$

2.4. а) $\begin{cases} x \equiv 3 (\mathrm{mod} 13), \\ x \equiv 5 (\mathrm{mod} 19), \\ x \equiv 8 (\mathrm{mod}\, 20), \\ x \equiv 13 (\mathrm{mod}\, 21). \end{cases}$ б) $\begin{cases} x \equiv 13 (\mathrm{mod}\, 25), \\ x \equiv 8 (\mathrm{mod}\, 29), \\ x \equiv 5 (\mathrm{mod}\, 22), \\ x \equiv 17 (\mathrm{mod}\, 24). \end{cases}$

2.5. а) $\begin{cases} x \equiv 1 (\mathrm{mod} 16), \\ x \equiv 6 (\mathrm{mod} 17), \\ x \equiv 9 (\mathrm{mod} 19), \\ x \equiv 5 (\mathrm{mod}\, 23). \end{cases}$ б) $\begin{cases} x \equiv 13 (\mathrm{mod} 18), \\ x \equiv 12 (\mathrm{mod} 17), \\ x \equiv 23 (\mathrm{mod}\, 26), \\ x \equiv 12 (\mathrm{mod} 19). \end{cases}$

2.6. а) $\begin{cases} x \equiv 4 (\mathrm{mod} 17), \\ x \equiv 17 (\mathrm{mod} 19), \\ x \equiv 0 (\mathrm{mod}\, 21), \\ x \equiv 10 (\mathrm{mod}\, 23). \end{cases}$ б) $\begin{cases} x \equiv 5 (\mathrm{mod}\, 77), \\ x \equiv 16 (\mathrm{mod} 19), \\ x \equiv 4 (\mathrm{mod}\, 35), \\ x \equiv 2 (\mathrm{mod} 13). \end{cases}$

2.7. а) $\begin{cases} x \equiv 3 (\mathrm{mod} 19), \\ x \equiv 8 (\mathrm{mod}\, 21), \\ x \equiv 2 (\mathrm{mod}\, 23), \\ x \equiv 4 (\mathrm{mod}\, 25). \end{cases}$ б) $\begin{cases} x \equiv 15 (\mathrm{mod}\, 23), \\ x \equiv 7 (\mathrm{mod}\, 20), \\ x \equiv 19 (\mathrm{mod}\, 21), \\ x \equiv 9 (\mathrm{mod}\, 46). \end{cases}$

2.8. а) $\begin{cases} x \equiv 5 (\mathrm{mod} 13), \\ x \equiv 9 (\mathrm{mod}\, 20), \\ x \equiv 20 (\mathrm{mod}\, 21), \\ x \equiv 8 (\mathrm{mod}\, 23). \end{cases}$ б) $\begin{cases} x \equiv 3 (\mathrm{mod}\, 29), \\ x \equiv 17 (\mathrm{mod} 19), \\ x \equiv 15 (\mathrm{mod}\, 23), \\ x \equiv 7 (\mathrm{mod}\, 38). \end{cases}$

2.9. а) $\begin{cases} x \equiv 16 (\mathrm{mod} 17), \\ x \equiv 17 (\mathrm{mod} 19), \\ x \equiv 9 (\mathrm{mod}\, 23), \\ x \equiv 17 (\mathrm{mod}\, 25). \end{cases}$ б) $\begin{cases} x \equiv 6 (\mathrm{mod}\, 29), \\ x \equiv 13 (\mathrm{mod}\, 34), \\ x \equiv 5 (\mathrm{mod}\, 23), \\ x \equiv 3 (\mathrm{mod}\, 32). \end{cases}$

2.10. а) $\begin{cases} x \equiv 14 (\mathrm{mod} 15), \\ x \equiv 16 (\mathrm{mod} 17), \\ x \equiv 15 (\mathrm{mod} 19), \\ x \equiv 3 (\mathrm{mod}\, 23). \end{cases}$ б) $\begin{cases} x \equiv 3 (\mathrm{mod}\, 31), \\ x \equiv 7 (\mathrm{mod}\, 33), \\ x \equiv 5 (\mathrm{mod}\, 34), \\ x \equiv 17 (\mathrm{mod}\, 36). \end{cases}$

2.11. а) $\begin{cases} x \equiv 6 (\mathrm{mod} 11), \\ x \equiv 0 (\mathrm{mod} 13), \\ x \equiv 16 (\mathrm{mod} 17), \\ x \equiv 11 (\mathrm{mod}\, 20). \end{cases}$ б) $\begin{cases} x \equiv 13 (\mathrm{mod}\, 25), \\ x \equiv 16 (\mathrm{mod}\, 27), \\ x \equiv 4 (\mathrm{mod}\, 29), \\ x \equiv 5 (\mathrm{mod}\, 20). \end{cases}$

2.12. а) $\begin{cases} x \equiv 3 (\mathrm{mod} 17), \\ x \equiv 17 (\mathrm{mod} 18), \\ x \equiv 16 (\mathrm{mod} 19), \\ x \equiv 9 (\mathrm{mod}\, 23). \end{cases}$ б) $\begin{cases} x \equiv 5 (\mathrm{mod}\, 37), \\ x \equiv 4 (\mathrm{mod}\, 39), \\ x \equiv 15 (\mathrm{mod}\, 29), \\ x \equiv 7 (\mathrm{mod} 18). \end{cases}$

2.13. а) $\begin{cases} x \equiv 8 (\mathrm{mod} 13), \\ x \equiv 5 (\mathrm{mod} 14), \\ x \equiv 12 (\mathrm{mod} 19), \\ x \equiv 20 (\mathrm{mod}\, 23). \end{cases}$ б) $\begin{cases} x \equiv 2 (\mathrm{mod}\, 33), \\ x \equiv 17 (\mathrm{mod}\, 31), \\ x \equiv 4 (\mathrm{mod} 15), \\ x \equiv 2 (\mathrm{mod}\, 29). \end{cases}$

2.14. а) $\begin{cases} x \equiv 6 (\mathrm{mod} 13), \\ x \equiv 3 (\mathrm{mod} 19), \\ x \equiv 3 (\mathrm{mod}\, 20), \\ x \equiv 5 (\mathrm{mod}\, 21). \end{cases}$ б) $\begin{cases} x \equiv 13 (\mathrm{mod}\, 35), \\ x \equiv 8 (\mathrm{mod}\, 49), \\ x \equiv 5 (\mathrm{mod}\, 21), \\ x \equiv 17 (\mathrm{mod}\, 44). \end{cases}$

2.15. а) $\begin{cases} x \equiv 5 (\mathrm{mod} 16), \\ x \equiv 4 (\mathrm{mod} 17), \\ x \equiv 4 (\mathrm{mod} 19), \\ x \equiv 13 (\mathrm{mod}\, 23). \end{cases}$ б) $\begin{cases} x \equiv 13 (\mathrm{mod}\, 28), \\ x \equiv 12 (\mathrm{mod}\, 37), \\ x \equiv 23 (\mathrm{mod}\, 36), \\ x \equiv 12 (\mathrm{mod}\, 59). \end{cases}$

2.16. а) $\begin{cases} x \equiv 6 (\mathrm{mod} 17), \\ x \equiv 17 (\mathrm{mod} 19), \\ x \equiv 19 (\mathrm{mod}\, 21), \\ x \equiv 6 (\mathrm{mod}\, 23). \end{cases}$ б) $\begin{cases} x \equiv 5 (\mathrm{mod}\, 57), \\ x \equiv 16 (\mathrm{mod}\, 39), \\ x \equiv 4 (\mathrm{mod}\, 55), \\ x \equiv 2 (\mathrm{mod} 13). \end{cases}$

2.17. а) $\begin{cases} x \equiv 1 (\mathrm{mod}\, 19), \\ x \equiv 4 (\mathrm{mod}\, 21), \\ x \equiv 19 (\mathrm{mod}\, 23), \\ x \equiv 21 (\mathrm{mod}\, 25). \end{cases}$ б) $\begin{cases} x \equiv 15 (\mathrm{mod}\, 43), \\ x \equiv 7 (\mathrm{mod}\, 30), \\ x \equiv 19 (\mathrm{mod}\, 41), \\ x \equiv 9 (\mathrm{mod}\, 56). \end{cases}$

2.18. а) $\begin{cases} x \equiv 7 (\mathrm{mod}\, 13), \\ x \equiv 11 (\mathrm{mod}\, 20), \\ x \equiv 1 (\mathrm{mod}\, 21), \\ x \equiv 10 (\mathrm{mod}\, 23). \end{cases}$ б) $\begin{cases} x \equiv 3 (\mathrm{mod}\, 59), \\ x \equiv 17 (\mathrm{mod}\, 29), \\ x \equiv 15 (\mathrm{mod}\, 22), \\ x \equiv 7 (\mathrm{mod}\, 34). \end{cases}$

2.19. а) $\begin{cases} x \equiv 13 (\mathrm{mod}\, 17), \\ x \equiv 16 (\mathrm{mod}\, 19), \\ x \equiv 12 (\mathrm{mod}\, 23), \\ x \equiv 22 (\mathrm{mod}\, 25). \end{cases}$ б) $\begin{cases} x \equiv 6 (\mathrm{mod}\, 49), \\ x \equiv 13 (\mathrm{mod}\, 35), \\ x \equiv 5 (\mathrm{mod}\, 33), \\ x \equiv 3 (\mathrm{mod}\, 52). \end{cases}$

2.20. а) $\begin{cases} x \equiv 6 (\mathrm{mod}\, 15), \\ x \equiv 6 (\mathrm{mod}\, 17), \\ x \equiv 3 (\mathrm{mod}\, 19), \\ x \equiv 10 (\mathrm{mod}\, 23). \end{cases}$ б) $\begin{cases} x \equiv 3 (\mathrm{mod}\, 41), \\ x \equiv 7 (\mathrm{mod}\, 53), \\ x \equiv 5 (\mathrm{mod}\, 54), \\ x \equiv 17 (\mathrm{mod}\, 38). \end{cases}$

Задание 3. Вычислить, используя различные методы возведения в степень.

3.1. а) $3925^{29575} (\mathrm{mod} 9859)$; б) $204^{162} (\mathrm{mod} 821)$; в) $43^{6890321} (\mathrm{mod} 8835)$.

3.2. а) $2529^{29659} (\mathrm{mod} 9887)$; б) $199^{158} (\mathrm{mod} 824)$; в) $56^{1893260} (\mathrm{mod} 7215)$.

3.3. а) $1204^{26420} (\mathrm{mod} 8807)$; б) $214^{149} (\mathrm{mod} 835)$; в) $49^{1763290} (\mathrm{mod} 4305)$.

3.4. а) $3529^{26209} (\mathrm{mod} 8737)$; б) $198^{179} (\mathrm{mod} 847)$; в) $61^{3873256} (\mathrm{mod} 6105)$.

3.5. а) $1501^{28388} (\mathrm{mod} 9463)$; б) $216^{182} (\mathrm{mod} 901)$; в) $54^{2237891} (\mathrm{mod} 6765)$.

3.6. а) $4523^{27449} (\mathrm{mod} 6863)$; б) $214^{181} (\mathrm{mod} 911)$; в) $48^{3763292} (\mathrm{mod} 6045)$.

3.7. а) $3922^{26833} (\mathrm{mod} 6709)$; б) $205^{178} (\mathrm{mod} 908)$; в) $44^{4674389} (\mathrm{mod} 7215)$.

3.8. а) $1063^{26930} (\mathrm{mod} 6733)$; б) $203^{152} (\mathrm{mod} 891)$; в) $57^{4782349} (\mathrm{mod} 4845)$.

3.9. а) $1125^{27794} (\mathrm{mod} 6949)$; б) $195^{154} (\mathrm{mod} 887)$; в) $50^{9001260} (\mathrm{mod} 5865)$.

3.10. а) $5205^{27113} (\mathrm{mod} 6779)$; б) $201^{167} (\mathrm{mod} 894)$; в) $62^{8750340} (\mathrm{mod} 7395)$.

3.11. а) $1308^{24176}(\mathrm{mod}\,8059)$; б) $202^{164}(\mathrm{mod}\,821)$; в) $55^{6964309}(\mathrm{mod}\,6545)$.

3.12. а) $6341^{24655}(\mathrm{mod}\,8219)$; б) $189^{159}(\mathrm{mod}\,824)$; в) $49^{5490752}(\mathrm{mod}\,7315)$.

3.13. а) $1423^{26822}(\mathrm{mod}\,8941)$; б) $213^{151}(\mathrm{mod}\,835)$; в) $45^{8652097}(\mathrm{mod}\,7735)$.

3.14. а) $5291^{27271}(\mathrm{mod}\,9091)$; б) $188^{197}(\mathrm{mod}\,847)$; в) $58^{6402380}(\mathrm{mod}\,8645)$.

3.15. а) $4922^{26239}(\mathrm{mod}\,8747)$; б) $217^{184}(\mathrm{mod}\,901)$; в) $51^{6079423}(\mathrm{mod}\,8855)$.

3.16. а) $1420^{24170}(\mathrm{mod}\,6043)$; б) $215^{183}(\mathrm{mod}\,911)$; в) $63^{7321907}(\mathrm{mod}\,4389)$.

3.17. а) $4524^{24045}(\mathrm{mod}\,6011)$; б) $206^{169}(\mathrm{mod}\,908)$; в) $56^{4567321}(\mathrm{mod}\,4641)$.

3.18. а) $3245^{29761}(\mathrm{mod}\,5953)$; б) $207^{148}(\mathrm{mod}\,891)$; в) $59^{2235647}(\mathrm{mod}\,5187)$.

3.19. а) $1224^{24026}(\mathrm{mod}\,6007)$; б) $196^{155}(\mathrm{mod}\,887)$; в) $46^{8943290}(\mathrm{mod}\,5313)$.

3.20. а) $4623^{24529}(\mathrm{mod}\,6133)$; б) $211^{169}(\mathrm{mod}\,894)$; в) $64^{6894320}(\mathrm{mod}\,6699)$.

Задание 4. Найти решения квадратичных сравнений.

4.1. а) $x^2 \equiv 326(\mathrm{mod}\,277)$; б) $x^2 \equiv 235(\mathrm{mod}\,563)$; в) $x^2 \equiv 127(\mathrm{mod}\,347)$;

г) $x^2 \equiv 52(\mathrm{mod}\,101)$; д) $x^2 \equiv 232(\mathrm{mod}\,313)$; е) $x^2 \equiv 13(\mathrm{mod}\,87)$.

4.2. а) $x^2 \equiv 266(\mathrm{mod}\,241)$; б) $x^2 \equiv 201(\mathrm{mod}\,227)$; в) $x^2 \equiv 70(\mathrm{mod}\,331)$;

г) $x^2 \equiv 83(\mathrm{mod}\,109)$; д) $x^2 \equiv 263(\mathrm{mod}\,281)$; е) $x^2 \equiv 28(\mathrm{mod}\,93)$.

4.3. а) $x^2 \equiv 333(\mathrm{mod}\,269)$; б) $x^2 \equiv 190(\mathrm{mod}\,223)$; в) $x^2 \equiv 113(\mathrm{mod}\,367)$;

г) $x^2 \equiv 24(\mathrm{mod}\,149)$; д) $x^2 \equiv 200(\mathrm{mod}\,257)$; е) $x^2 \equiv 34(\mathrm{mod}\,55)$.

4.4. а) $x^2 \equiv 388(\mathrm{mod}\,307)$; б) $x^2 \equiv 296(\mathrm{mod}\,463)$; в) $x^2 \equiv 97(\mathrm{mod}\,283)$;

г) $x^2 \equiv 42(\mathrm{mod}\,157)$; д) $x^2 \equiv 236(\mathrm{mod}\,241)$; е) $x^2 \equiv 39(\mathrm{mod}\,65)$.

4.5. а) $x^2 \equiv 306(\mathrm{mod}\,281)$; б) $x^2 \equiv 309(\mathrm{mod}\,467)$; в) $x^2 \equiv 182(\mathrm{mod}\,359)$;

г) $x^2 \equiv 78(\mathrm{mod}\,173)$; д) $x^2 \equiv 66(\mathrm{mod}\,233)$; е) $x^2 \equiv 26(\mathrm{mod}\,85)$.

4.6. а) $x^2 \equiv 307(\mathrm{mod}\,149)$; б) $x^2 \equiv 79(\mathrm{mod}\,523)$; в) $x^2 \equiv 91(\mathrm{mod}\,431)$;

г) $x^2 \equiv 34(\mathrm{mod}\,181)$; д) $x^2 \equiv 134(\mathrm{mod}\,193)$; е) $x^2 \equiv 35(\mathrm{mod}\,95)$.

4.7. а) $x^2 \equiv 354(\mathrm{mod}\,127)$; б) $x^2 \equiv 356(\mathrm{mod}\,547)$; в) $x^2 \equiv 138(\mathrm{mod}\,439)$;

г) $x^2 \equiv 24 (\mathrm{mod} 197)$; д) $x^2 \equiv 11 (\mathrm{mod} 137)$; е) $x^2 \equiv 42 (\mathrm{mod} 77)$.

4.8. а) $x^2 \equiv 343 (\mathrm{mod} 131)$; б) $x^2 \equiv 220 (\mathrm{mod} 251)$; в) $x^2 \equiv 137 (\mathrm{mod} 419)$;

г) $x^2 \equiv 80 (\mathrm{mod} 229)$; д) $x^2 \equiv 7 (\mathrm{mod} 113)$; е) $x^2 \equiv 78 (\mathrm{mod} 91)$.

4.9. а) $x^2 \equiv 378 (\mathrm{mod} 157)$; б) $x^2 \equiv 191 (\mathrm{mod} 239)$; в) $x^2 \equiv 243 (\mathrm{mod} 443)$;

г) $x^2 \equiv 93 (\mathrm{mod} 269)$; д) $x^2 \equiv 95 (\mathrm{mod} 97)$; е) $x^2 \equiv 6 (\mathrm{mod} 69)$.

4.10. а) $x^2 \equiv 379 (\mathrm{mod} 149)$; б) $x^2 \equiv 260 (\mathrm{mod} 271)$; в) $x^2 \equiv 125 (\mathrm{mod} 479)$;

г) $x^2 \equiv 71 (\mathrm{mod} 277)$; д) $x^2 \equiv 11 (\mathrm{mod} 89)$; е) $x^2 \equiv 7 (\mathrm{mod} 57)$.

4.11. а) $x^2 \equiv 420 (\mathrm{mod} 137)$; б) $x^2 \equiv 235 (\mathrm{mod} 479)$; в) $x^2 \equiv 245 (\mathrm{mod} 271)$;

г) $x^2 \equiv 97 (\mathrm{mod} 101)$; д) $x^2 \equiv 137 (\mathrm{mod} 313)$; е) $x^2 \equiv 52 (\mathrm{mod} 87)$.

4.12. а) $x^2 \equiv 496 (\mathrm{mod} 157)$; б) $x^2 \equiv 205 (\mathrm{mod} 443)$; в) $x^2 \equiv 15 (\mathrm{mod} 239)$;

г) $x^2 \equiv 28 (\mathrm{mod} 109)$; д) $x^2 \equiv 28 (\mathrm{mod} 281)$; е) $x^2 \equiv 82 (\mathrm{mod} 93)$.

4.13. а) $x^2 \equiv 442 (\mathrm{mod} 139)$; б) $x^2 \equiv 193 (\mathrm{mod} 419)$; в) $x^2 \equiv 68 (\mathrm{mod} 251)$;

г) $x^2 \equiv 110 (\mathrm{mod} 149)$; д) $x^2 \equiv 122 (\mathrm{mod} 257)$; е) $x^2 \equiv 14 (\mathrm{mod} 55)$.

4.14. а) $x^2 \equiv 420 (\mathrm{mod} 113)$; б) $x^2 \equiv 296 (\mathrm{mod} 439)$; в) $x^2 \equiv 165 (\mathrm{mod} 547)$;

г) $x^2 \equiv 145 (\mathrm{mod} 157)$; д) $x^2 \equiv 82 (\mathrm{mod} 241)$; е) $x^2 \equiv 61 (\mathrm{mod} 65)$.

4.15. а) $x^2 \equiv 637 (\mathrm{mod} 211)$; б) $x^2 \equiv 309 (\mathrm{mod} 431)$; в) $x^2 \equiv 13 (\mathrm{mod} 523)$;

г) $x^2 \equiv 140 (\mathrm{mod} 173)$; д) $x^2 \equiv 117 (\mathrm{mod} 233)$; е) $x^2 \equiv 55 (\mathrm{mod} 85)$.

4.16. а) $x^2 \equiv 210 (\mathrm{mod} 89)$; б) $x^2 \equiv 83 (\mathrm{mod} 359)$; в) $x^2 \equiv 165 (\mathrm{mod} 467)$;

г) $x^2 \equiv 13 (\mathrm{mod} 181)$; д) $x^2 \equiv 118 (\mathrm{mod} 193)$; е) $x^2 \equiv 6 (\mathrm{mod} 95)$.

4.17. а) $x^2 \equiv 227 (\mathrm{mod} 83)$; б) $x^2 \equiv 56 (\mathrm{mod} 283)$; в) $x^2 \equiv 194 (\mathrm{mod} 463)$;

г) $x^2 \equiv 96 (\mathrm{mod} 197)$; д) $x^2 \equiv 115 (\mathrm{mod} 137)$; е) $x^2 \equiv 15 (\mathrm{mod} 77)$.

4.18. а) $x^2 \equiv 248 (\mathrm{mod} 79)$; б) $x^2 \equiv 221 (\mathrm{mod} 367)$; в) $x^2 \equiv 217 (\mathrm{mod} 223)$;

г) $x^2 \equiv 85 (\mathrm{mod} 229)$; д) $x^2 \equiv 69 (\mathrm{mod} 113)$; е) $x^2 \equiv 53 (\mathrm{mod} 91)$.

4.19. а) $x^2 \equiv 197 (\mathrm{mod} 97)$; б) $x^2 \equiv 192 (\mathrm{mod} 331)$; в) $x^2 \equiv 44 (\mathrm{mod} 227)$;

г) $x^2 \equiv 47 (\mathrm{mod} 269)$; д) $x^2 \equiv 50 (\mathrm{mod} 97)$; е) $x^2 \equiv 52 (\mathrm{mod} 69)$.

4.20. а) $x^2 \equiv 298 (\mathrm{mod}\, 73)$; б) $x^2 \equiv 260 (\mathrm{mod}\, 347)$; в) $x^2 \equiv 545 (\mathrm{mod}\, 563)$;

г) $x^2 \equiv 189 (\mathrm{mod}\, 277)$; д) $x^2 \equiv 44 (\mathrm{mod}\, 89)$; е) $x^2 \equiv 43 (\mathrm{mod}\, 57)$.

Задание 5. Найти первообразный корень по модулю m.

5.1. а) $m = 233$; б) $m = 3125$; в) $m = 8978$.

5.2. а) $m = 197$; б) $m = 2401$; в) $m = 7442$.

5.3. а) $m = 239$; б) $m = 6561$; в) $m = 6962$.

5.4. а) $m = 199$; б) $m = 1331$; в) $m = 5618$.

5.5. а) $m = 241$; б) $m = 2197$; в) $m = 4418$.

5.6. а) $m = 317$; б) $m = 4913$; в) $m = 3698$.

5.7. а) $m = 251$; б) $m = 12167$; в) $m = 3362$.

5.8. а) $m = 313$; б) $m = 24389$; в) $m = 2738$.

5.9. а) $m = 257$; б) $m = 14641$; в) $m = 1922$.

5.10. а) $m = 211$; б) $m = 19683$; в) $m = 1682$.

5.11. а) $m = 263$; б) $m = 2187$; в) $m = 1058$.

5.12. а) $m = 311$; б) $m = 16807$; в) $m = 722$.

5.13. а) $m = 269$; б) $m = 15625$; в) $m = 578$.

5.14. а) $m = 307$; б) $m = 29791$; в) $m = 4394$.

5.15. а) $m = 271$; б) $m = 6241$; в) $m = 2662$.

5.16. а) $m = 293$; б) $m = 6889$; в) $m = 4802$.

5.17. а) $m = 277$; б) $m = 7921$; в) $m = 686$.

5.18. а) $m = 283$; б) $m = 9409$; в) $m = 6250$.

5.19. а) $m = 223$; б) $m = 10201$; в) $m = 1458$.

5.20. а) $m = 281$; б) $m = 10609$; в) $m = 486$.

Задание 6. Составить таблицу индексов по модулю *p*. Используя данную таблицу, решить сравнения.

6.1. p=23; а) $17x \equiv 14 (\mathrm{mod}\, 23)$; б) $x^3 \equiv 20 (\mathrm{mod}\, 23)$.

6.2. p=29; а) $15x \equiv 11 (\mathrm{mod}\, 29)$; б) $x^3 \equiv 14 (\mathrm{mod}\, 29)$.

6.3. p=31; а) $17x \equiv 12 (\mathrm{mod}\, 31)$; б) $x^3 \equiv 16 (\mathrm{mod}\, 31)$.

6.4. p=19; а) $18x \equiv 7 (\mathrm{mod}\, 19)$; б) $x^3 \equiv 18 (\mathrm{mod}\, 19)$.

6.5. p=17; а) $13x \equiv 9 (\mathrm{mod}\, 17)$; б) $x^3 \equiv 3 (\mathrm{mod}\, 17)$.

6.6. p=23; а) $15x \equiv 8 (\mathrm{mod}\, 23)$; б) $x^4 \equiv 8 (\mathrm{mod}\, 23)$.

6.7. p=29; а) $16x \equiv 9 (\mathrm{mod}\, 29)$; б) $x^4 \equiv 20 (\mathrm{mod}\, 29)$.

6.8. p=31; а) $12x \equiv 5 (\mathrm{mod}\, 31)$; б) $x^4 \equiv 5 (\mathrm{mod}\, 31)$.

6.9. p=19; а) $13x \equiv 10 (\mathrm{mod}\, 19)$; б) $x^4 \equiv 17 (\mathrm{mod}\, 19)$.

6.10. p=17; а) $11x \equiv 3 (\mathrm{mod}\, 17)$; б) $x^4 \equiv 13 (\mathrm{mod}\, 17)$.

6.11. p=23; а) $19x \equiv 13 (\mathrm{mod}\, 23)$; б) $x^5 \equiv 12 (\mathrm{mod}\, 23)$.

6.12. p=29; а) $21x \equiv 4 (\mathrm{mod}\, 29)$; б) $x^5 \equiv 11 (\mathrm{mod}\, 29)$.

6.13. p=31; а) $11x \equiv 5 (\mathrm{mod}\, 31)$; б) $x^5 \equiv 26 (\mathrm{mod}\, 31)$.

6.14. p=19; а) $10x \equiv 3 (\mathrm{mod}\, 19)$; б) $x^5 \equiv 13 (\mathrm{mod}\, 19)$.

6.15. p=17; а) $6x \equiv 13 (\mathrm{mod}\, 17)$; б) $x^5 \equiv 15 (\mathrm{mod}\, 17)$.

6.16. p=23; а) $8x \equiv 15 (\mathrm{mod}\, 23)$; б) $x^6 \equiv 18 (\mathrm{mod}\, 23)$.

6.17. p=29; а) $20x \equiv 3 (\mathrm{mod}\, 29)$; б) $x^6 \equiv 6 (\mathrm{mod}\, 29)$.

6.18. p=31; а) $9x \equiv 20 (\mathrm{mod}\, 31)$; б) $x^6 \equiv 2 (\mathrm{mod}\, 31)$.

6.19. p=19; а) $3x \equiv 11 (\mathrm{mod}\, 19)$; б) $x^6 \equiv 7 (\mathrm{mod}\, 19)$.

6.20. p=17; а) $4x \equiv 11 (\mathrm{mod}\, 17)$; б) $x^6 \equiv 15 (\mathrm{mod}\, 17)$.

Задание 7. Известен модуль n и шифрующая экспонента e алгоритма *RSA*. Зашифровать указанную букву русского алфавита, при условии, что рассматривается алфавит из 33 букв, нумерация букв алфавите начинается с 1.

7.1. n=41273, e=23, буква «П».

7.2. n=37901, e=29, буква «С».

7.3. n=36031, e=31, буква «Р».

7.4. n=40379, e=19, буква «Т».

7.5. n=35723, e=37, буква «Ф».

7.6. n=47897, e=17, буква «У».

7.7. n=45571, e=23, буква «Ц».

7.8. n=43139, e=29, буква «Ч».

7.9. n=45901, e=31, буква «Х».

7.10. n=40729, e=19, буква «Щ».

7.11. n=41273, e=37, буква «Ъ».

7.12. n=37901, e=17, буква «Ш».

7.13. n=36031, e=23, буква «Ь».

7.14. n=40379, e=29, буква «Ю».

7.15. n=35723, e=31, буква «Я».

7.16. n=47897, e=19, буква «Э».

7.17. n=45571, e=37, буква «Н».

7.18. n=43139, e=17, буква «М».

7.19. n=45901, e=23, буква «Л».

7.20. n=40729, e=29, буква «К».

Задание 8. Найти секретный ключ d алгоритма *RSA*, если известен модуль n и открытый ключ e.

8.1. n=16259, e=43.

8.2. n=16013, e=41.

8.3. n=13303, e=47.

8.4. n=15517, e=37.

8.5. n=15403, e=31.

8.6. n=15721, e=53.

8.7. n=17533, e=59.

8.8. n=14359, e=29.

8.9. n=14701, e=23.

8.10. n=12319, e=19.

8.11. n=16259, e=29.

8.12. n=16013, e=23.

8.13. n=13303, e=19.

8.14. n=15517, e=59.

8.15. n=15403, e=53.

8.16. n=15721, e=31.

8.17. n=17533, e=37.

8.18. n=14359, e=47.

8.19. n=14701, e=41.

8.20. n=12319, e=43.

Задание 9. Проверить подлинность сообщения m с цифровой подписью s от отправителя, шифрующая экспонента которого равна e, а модуль алгоритма *RSA* – n.

9.1. m=525, s=197, e=37, n=3053.

9.2. m=461, s=2474, e=31, n=2881.

9.3. m=359 , s=332, e=29, n=2747.

9.4. m=426, s=426, e=41, n=2911.

9.5. m=622, s=1453, e=43, n=2491.

9.6. m=362, s=2745, e=19, n=2773.

9.7. m=445, s=38, e=23, n=2627.

9.8. m=392, s=1633, e=17, n=2701.

9.9. m=472, s=2180, e=47, n=2449.

9.10. m=502, s=1979, e=53, n=2263.

9.11. m=502, s=664, e=53, n=3053.

9.12. m=472, s=2063, e=47, n=2881.

9.13. m=392, s=2245, e=17, n=2747.

9.14. m=445, s=1529, e=23, n=2911.

9.15. m=362, s=301, e=19, n=2491.

9.16. m=622, s=1312, e=43, n=2773.

9.17. m=426, s=1349, e=41, n=2627.

9.18. m=359, s=1860, e=29, n=2701.

9.19. m=461, s=1298, e=31, n=2449.

9.20. m=525, s=643, e=37, n=2263.

Задание 10. Решить задачу о безопасном хранении ключа K, если любые L из N человек, получивших информацию о ключе, могли бы вместе восстановить ключ, но $L' < L$ человек не смогли бы этого сделать. Показать процедуру восстановления ключа, выбрав части ключа произвольным образом.

10.1. K=11, L=3, N=4.

10.2. K=9, L=4, N=5.

10.3. K=10, L=3, N=6.

10.4. K=8, L=3, N=5.

10.5. K=9, L=4, N=6.

10.6. K=12, L=3, N=4.

10.7. K=13, L=4, N=5.

10.8. K=11, L=3, N=6.

10.9. K=9, L=3, N=5.

10.10. K=8, L=4, N=6.

10.11. K=10, L=3, N=4.

10.12. K=12, L=4, N=5.

10.13. K=13, L=3, N=6.

10.14. K=11, L=3, N=5.

10.15. K=9, L=4, N=7.

10.16. K=12, L=3, N=7.

10.17. K=8, L=3, N=4.

10.18. K=10, L=4, N=5.

10.19. K=13, L=3, N=5.

10.20. K=11, L=4, N=7.

2 Решение типового варианта расчетно-графического задания

Задание 1. Решить следующие сравнения:

а) $4326x \equiv 167 (\mathrm{mod}\, 821)$; б) $4895x \equiv 745 (\mathrm{mod}\, 5280)$; в) $1326x \equiv 3672 (\mathrm{mod}\, 3534)$.

Решение.

а) Решим сравнение

$$4326x \equiv 167 (\mathrm{mod}\, 821). \quad (1)$$

Заметим, что $4326 \equiv 221 (\mathrm{mod}\, 821)$. Поэтому вместо исходного сравнения можно решать сравнение

$$221x \equiv 167 (\mathrm{mod}\, 821). \quad (2)$$

Выясним, имеет ли оно решения.

Напомним, что сравнение $ax \equiv b (\mathrm{mod}\, m)$, где $a, b, m \in Z$, $m > 1$, имеет решение тогда и только тогда, когда *НОД(a,b)|c*. Если решения сравнения существуют, то их количество в кольце Z_m равно *d = НОД(a,b)*.

Найдем *НОД*(221,821), используя расширенный алгоритм Евклида. Вычисления оформим в таблице 1.

Таблица 1 – Поиск *НОД*(221,821) и его линейного представления.

i	a_i	x_i	y_i	q_i
0	821	1	0	-
1	221	0	1	3
2	158	1	–3	1
3	63	–1	4	2
4	32	3	–11	1
5	31	–4	15	1
6	1	7	–26	31
7	0			

Получили *НОД*(221,821) = 1. Так как 1|167, то сравнение имеет решения. В кольце Z_{821} сравнение имеет единственное решение. Найдем его. Для этого умножим обе части сравнения (2) на $221^{-1}(\mathrm{mod}821)$. Получим $x \equiv 221^{-1} \cdot 167(\mathrm{mod}821)$.

Найдем $221^{-1}(\mathrm{mod}821)$. Для этого воспользуемся линейным представлением *НОД*(221,821). Коэффициенты линейного представления были найдены при вычислении *НОД*(221,821) с помощью расширенного алгоритма Евклида: $НОД(221,821) = -26 \cdot 221 + 7 \cdot 821$. Тогда $221^{-1}(\mathrm{mod}821) = -26$ или $221^{-1}(\mathrm{mod}821) = 795$.

Получаем $x \equiv -26 \cdot 167 \equiv 584(\mathrm{mod}821)$. В кольце Z_{821} сравнение (2) имеет единственное решение $x = 584$.

Ответ: $x \equiv 584(\mathrm{mod}821)$.

б) Выясним, имеет ли решения сравнение

$$4895x \equiv 745(\mathrm{mod}5280). \qquad (3)$$

Найдем *НОД*(4895,5280), используя алгоритм Евклида.

НОД(5280, 4895) = *НОД*(4895, 385) = *НОД*(385, 275) = *НОД*(275, 110) = = *НОД*(110, 55) = *НОД*(55, 0) = 55.

Так как 55 не делит число 745, то сравнение (3) решений не имеет.

Ответ: решений нет.

в) Решим сравнение

$$1326x \equiv 3672(\mathrm{mod}3534). \qquad (4)$$

Заметим, что $3672 \equiv 138(\mathrm{mod}3534)$. Поэтому вместо исходного сравнения можно решать сравнение

$$1326x \equiv 138(\mathrm{mod}3534). \qquad (5)$$

Выясним, имеет ли оно решения.

Находим *НОД*(3534,1326) = *НОД*(1326,882) = *НОД*(882,444) = *НОД*(444,438) = = *НОД*(438,6) = *НОД*(6,0) = 6.

Так как 6|138, то сравнение (5) имеет решения. В кольце Z_{3534} сравнение (5) имеет 6 решений.

Разделим обе части сравнения (5) и его модуль на *НОД*(3534,1326) = 6. Получим сравнение:

$$221x \equiv 23 (\mathrm{mod}\, 589). \qquad (6)$$

НОД(221,589) = 1, то есть сравнение (6) имеет единственное решение в кольце Z_{589}, которое найдем как $x \equiv 221^{-1} \cdot 23 (\mathrm{mod}\, 589)$.

$221^{-1} (\mathrm{mod}\, 589)$ найдем, используя расширенный алгоритма Евклида, вычисления согласно которому представлены в таблице 2. Так как $НОД(221,589) = 8 \cdot 221 + (-3) \cdot 589$, то $221^{-1} (\mathrm{mod}\, 589) = 8$.

Таблица 2 – Поиск *НОД*(221,589) и его линейного представления.

i	a_i	x_i	y_i	q_i
0	589	1	0	-
1	221	0	1	2
2	147	1	–2	1
3	74	–1	3	1
4	73	2	–5	1
5	1	–3	8	73
6	0			

Находим решение сравнения (6): $x \equiv 8 \cdot 23 (\mathrm{mod}\, 589) \equiv 184 (\mathrm{mod}\, 589)$. Решение $x = 184$ является единственным в кольце Z_{589}.

В кольце целых чисел решений сравнения (4) бесконечно много и их можно представить в виде

$$x = 184 + 589k,\ k \in Z. \qquad (7)$$

В кольце Z_{3534} решений сравнения (4) всего шесть и они находятся по формуле (7) при $k = \overline{0,5}$, то есть решениями будут $x = 184, 773, 1362, 1951, 2540, 3129$.

Ответ: $x \equiv 184 (\mathrm{mod}\, 589)$.

Задание 2. Найти решения систем линейных сравнений, используя греко-китайскую теорему об остатках:

а) $\begin{cases} x \equiv 3(\mathrm{mod}\, 5), \\ x \equiv 6(\mathrm{mod}\, 13), \\ x \equiv 4(\mathrm{mod}\, 11), \\ x \equiv 7(\mathrm{mod}\, 9). \end{cases}$; б) $\begin{cases} x \equiv 3(\mathrm{mod}\, 5), \\ x \equiv 6(\mathrm{mod}\, 7), \\ x \equiv 4(\mathrm{mod}\, 9), \\ x \equiv 2(\mathrm{mod}\, 12). \end{cases}$

Решение.

а) Решим систему сравнений

$$\begin{cases} x \equiv 3(\mathrm{mod}\, 5), \\ x \equiv 6(\mathrm{mod}\, 13), \\ x \equiv 4(\mathrm{mod}\, 11), \\ x \equiv 7(\mathrm{mod}\, 9). \end{cases} \qquad (8)$$

Выясним, удовлетворяет ли данная система условиям греко-китайской теоремы об остатках. Для этого необходимо проверить, являются ли модули сравнений, входящих в систему (8), попарно взаимно простыми числами. Так как $НОД(5,13) = НОД(5,11) = НОД(5,9) = НОД(13,11) = НОД(13,9) = НОД(11,9) = 1,$ то система сравнений имеет решения, причем в кольце целых чисел таких решений бесконечно много, а в кольце Z_{1485} система (8) имеет единственное решение.

Итак, необходимо найти значение *x*, удовлетворяющее всем сравнениям системы (8). Из первого сравнения системы $x \equiv 3(\mathrm{mod}\, 5)$ следует, что $x = 3 + 5k,\ k \in Z$. Чтобы найти *k*, подставим *x* во второе сравнение: $3 + 5k \equiv 6(\mathrm{mod}13)$ или $5k \equiv 3(\mathrm{mod}13)$. Так как $5^{-1} \equiv 8(\mathrm{mod}13)$, то $k \equiv 5^{-1} \cdot 3(\mathrm{mod}13) \equiv 8 \cdot 3(\mathrm{mod}13) \equiv 11(\mathrm{mod}13)$ или $k = 11 + 13t,\ t \in Z$. Следовательно, решением системы из первых двух сравнений является $x = 3 + 5(11 + 13t) = 58 + 65t, t \in Z$, то есть $x \equiv 58(\mathrm{mod}\, 65)$.

Находим значение *x*, удовлетворяющее сравнению $x \equiv 58(\mathrm{mod}\, 65)$ и третьему сравнению системы (8). Имеем $x = 58 + 65t \equiv 4(\mathrm{mod}11)$ или $65t \equiv (4 - 58)(\mathrm{mod}11) \equiv -54(\mathrm{mod}11)$. Так как $65 \equiv -1(\mathrm{mod}11)$, а $-54 \equiv -10(\mathrm{mod}11)$, то

$-t \equiv -10(\mathrm{mod}11)$ или $t \equiv 10(\mathrm{mod}11)$. Следовательно, $t = 10 + 11p,\ p \in Z$, и решением системы из первых трех сравнений является $x = 58 + 65(10 + 11p) = 708 + 715p,\ p \in Z$, то есть $x \equiv 708(\mathrm{mod}715)$.

Находим x, удовлетворяющее сравнению $x \equiv 708(\mathrm{mod}715)$ и четвертому сравнению системы (8). Имеем $x = 708 + 715p \equiv 7(\mathrm{mod}9)$ или $715p \equiv -701(\mathrm{mod}9)$. Так как $715 \equiv 4(\mathrm{mod}9)$, а $-701 \equiv 1(\mathrm{mod}9)$, то $4p \equiv 1(\mathrm{mod}9)$ или $p \equiv 4^{-1}(\mathrm{mod}9) \equiv 7(\mathrm{mod}9)$. Следовательно, $p = 7 + 9n,\ n \in Z$, и решением системы из четырех сравнений является $x = 708 + 715(7 + 9n) = 5713 + 6435n,\ n \in Z$, то есть $x \equiv 5713(\mathrm{mod}6435)$. Это и есть решение системы (8).

Ответ: $x \equiv 5713(\mathrm{mod}6435)$.

б) Выясним, можно ли воспользоваться греко-китайской теоремой об остатках для системы сравнений

$$\begin{cases} x \equiv 3(\mathrm{mod}5), \\ x \equiv 6(\mathrm{mod}7), \\ x \equiv 4(\mathrm{mod}9), \\ x \equiv 2(\mathrm{mod}12). \end{cases} \qquad (9)$$

Так как НОД(9,12) = 3, то модули системы не являются попарно взаимно простыми, поэтому найти решение, используя греко-китайскую теорему об остатках, нельзя.

Задание 3. Найти: а) $4875^{18442}(\mathrm{mod}9221)$; б) $144^{183}(\mathrm{mod}925)$; в) $43^{674389}(\mathrm{mod}5005)$.

Решение.

а) По таблице простых чисел (приложение А) определяем, что 9221 является простым числом, НОД(4875, 9221) = 1. По теореме Ферма $4875^{9219} \equiv 1(\mathrm{mod}9221)$. Так как $18442 = 9219 \cdot 2 + 4$, то

$$4875^{18442}(\mathrm{mod}9221) \equiv 4875^{9219\cdot 2+4}(\mathrm{mod}9221) \equiv (4875^{9219})^2 4875^4(\mathrm{mod}9221) \equiv$$
$$\equiv 4875^4(\mathrm{mod}9221) \equiv (4875^2)^2(\mathrm{mod}9221) \equiv (23765625)^2(\mathrm{mod}9221) \equiv$$
$$\equiv (3108)^2(\mathrm{mod}9221) \equiv 9659664(\mathrm{mod}9221) \equiv 5277.$$

Ответ: 5277.

б) Для вычисления $144^{183}(\mathrm{mod}925)$ воспользуемся бинарным (индийским) методом возведения в степень.

Находим представление числа 183 в двоичной системе счисления:

$183_{10} = 10110111_2$.

Формируем правило возведения в степень. Заменим каждую цифру «1» на пару букв «SM_{144}» и каждую цифру «0» на букву «S», получим последовательность «$SM_{144}SSM_{144}SM_{144}SSM_{144}SM_{144}SM_{144}$». Теперь вычеркнем пару букв «SM_{144}» слева. Получившаяся последовательность букв «$SSM_{144}SM_{144}SSM_{144}SM_{144}SM_{144}$» представляет собой правило для вычисления $144^{183}(\mathrm{mod}925)$, если интерпретировать «S» как «возвести в квадрат и взять остаток по модулю 925», а «M_{144}» как «умножить на 144 и взять остаток по модулю 925».

Проводя вычисления последовательно, получим следующие результаты:

$144^2(\mathrm{mod}925) \equiv 386(\mathrm{mod}925)$,

$386^2(\mathrm{mod}925) \equiv 71(\mathrm{mod}925)$,

$71 \cdot 144(\mathrm{mod}925) \equiv 49(\mathrm{mod}925)$,

$49^2(\mathrm{mod}925) \equiv 551(\mathrm{mod}925)$,

$551 \cdot 144(\mathrm{mod}925) \equiv 719(\mathrm{mod}925) \equiv -206(\mathrm{mod}925)$,

$(-206)^2(\mathrm{mod}925) \equiv 811(\mathrm{mod}925) \equiv -114(\mathrm{mod}925)$,

$(-114)^2(\mathrm{mod}925) \equiv 46(\mathrm{mod}925)$,

$46 \cdot 144(\mathrm{mod}925) \equiv 149(\mathrm{mod}925)$,

$149^2(\mathrm{mod}925) \equiv 1(\mathrm{mod}925)$,

$1 \cdot 144(\mathrm{mod}925) = 144$,

$144^2(\mathrm{mod}925) \equiv 386(\mathrm{mod}925)$,

$386 \cdot 144(\mathrm{mod}925) \equiv 84(\mathrm{mod}925)$.

Ответ: 84.

в) Так как в данном случае модуль 5005 раскладывается на сравнительно небольшие простые делители, то есть $5005 = 5 \cdot 7 \cdot 11 \cdot 13$, то для вычисления $43^{674389} (\mathrm{mod} 5005)$ воспользуемся греко-китайской теоремой об остатках.

Найдем $43^{674389} (\mathrm{mod} 5) \equiv 3^{674389} (\mathrm{mod} 5)$. По теореме Ферма $3^4 \equiv 1 (\mathrm{mod} 5)$. Так как $674389 = 168597 \cdot 4 + 1$, то $3^{674389} (\mathrm{mod} 5) \equiv 3^{4 \cdot 168597 + 1} (\mathrm{mod} 5) \equiv (3^4)^{168597} \cdot 3 (\mathrm{mod} 5) \equiv$ $\equiv 3 (\mathrm{mod} 5)$.

В случае простого модуля 7 получаем $43^{674389} (\mathrm{mod} 7) \equiv 1 (\mathrm{mod} 7)$.

Рассматривая простой модуль 11, заметим, что $43 (\mathrm{mod} 11) \equiv 10 (\mathrm{mod} 11) \equiv -1 (\mathrm{mod} 11)$. Тогда $43^{674389} (\mathrm{mod} 11) \equiv (-1)^{674389} (\mathrm{mod} 11) \equiv$ $\equiv (-1)^{674388+1} (\mathrm{mod} 11) \equiv (-1)^{674388} \cdot (-1) (\mathrm{mod} 11) \equiv -1 (\mathrm{mod} 11) \equiv 10 (\mathrm{mod} 11)$.

Наконец, в случае модуля 13, получаем $43^{674389} (\mathrm{mod} 13) \equiv 4^{674389} (\mathrm{mod} 13)$. По теореме Ферма $4^{12} \equiv 1 (\mathrm{mod} 13)$. Так как $674389 = 56199 \cdot 12 + 1$, то $4^{674389} (\mathrm{mod} 13) \equiv 4^{12 \cdot 56199 + 1} (\mathrm{mod} 13) \equiv (4^{12})^{56199} \cdot 4 (\mathrm{mod} 13) \equiv 4 (\mathrm{mod} 13)$.

Итак, $43^{674389} \equiv 3 (\mathrm{mod} 5)$, $43^{674389} \equiv 1 (\mathrm{mod} 5)$, $43^{674389} \equiv 10 (\mathrm{mod} 11)$, $4^{674389} \equiv 4 (\mathrm{mod} 13)$. Введем обозначение $43^{674389} = x$ и получим систему линейных сравнений с одним неизвестным:

$$\begin{cases} x \equiv 3 (\mathrm{mod} 5), \\ x \equiv 1 (\mathrm{mod} 7), \\ x \equiv 10 (\mathrm{mod} 11), \\ x \equiv 4 (\mathrm{mod} 13). \end{cases} \qquad (10)$$

Система (10) имеет единственное решение в кольце $\mathbb{Z}_{5005}$. Найдем это решение.

Из первого сравнения системы $x \equiv 3 (\mathrm{mod} 5)$ следует, что $x = 3 + 5k, k \in Z$. Чтобы найти k, подставим x во второе сравнение: $3 + 5k \equiv 1 (\mathrm{mod} 7)$ или $5k \equiv -2 (\mathrm{mod} 7)$. Так как $-2 \equiv 5 (\mathrm{mod} 7)$, то последнее сравнение примет вид $5k \equiv 5 (\mathrm{mod} 7)$, обе части которого разделим на 5 и получим, что $k \equiv 1 (\mathrm{mod} 7)$ или

$k = 1 + 7t,\ t \in Z$. Следовательно, решением системы из первых двух сравнений является $x = 3 + 5(1 + 7t) = 8 + 35t,\ t \in Z$, то есть $x \equiv 58(\mathrm{mod}\,65)$.

Находим значение x, удовлетворяющее сравнению $x \equiv 8(\mathrm{mod}\,35)$ и третьему сравнению системы (10). Имеем $x = 8 + 35t \equiv 10(\mathrm{mod}\,11)$ или $35t \equiv 2(\mathrm{mod}\,11)$. Так как $35 \equiv 2(\mathrm{mod}\,11)$, то $2t \equiv 2(\mathrm{mod}\,11)$ или $t \equiv 1(\mathrm{mod}\,11)$. Следовательно, $t = 1 + 11p,\ p \in Z$, и решением системы из первых трех сравнений является $x = 8 + 35(1 + 11p) = 43 + 385p,\ p \in Z$, то есть $x \equiv 43(\mathrm{mod}\,385)$.

Находим x, удовлетворяющее сравнению $x \equiv 43(\mathrm{mod}\,385)$ и четвертому сравнению системы (10). Имеем $x = 43 + 385p \equiv 4(\mathrm{mod}\,13)$ или $385p \equiv -39(\mathrm{mod}\,13)$. Так как $-39 \equiv 0(\mathrm{mod}\,13)$, то $p \equiv 0(\mathrm{mod}\,13)$. Следовательно, $p = 13n,\ n \in Z$, и решением системы из четырех сравнений является $x = 43 + 385(13n) = 43 + 5005n,\ n \in Z$, то есть $x \equiv 43(\mathrm{mod}\,5005)$. Это и есть решение системы (10). Так как $x = 43^{674389}$, то $43^{674389}(\mathrm{mod}\,5005) = 43$.

Ответ: 43.

Задание 4. Найти решения квадратичных сравнений:

а) $x^2 \equiv 207(\mathrm{mod}\,191)$; б) $x^2 \equiv 188(\mathrm{mod}\,263)$; в) $x^2 \equiv 146(\mathrm{mod}\,311)$; г) $x^2 \equiv 34(\mathrm{mod}\,61)$;

д) $x^2 \equiv 62(\mathrm{mod}\,97)$; е) $x^2 \equiv 145(\mathrm{mod}\,51)$.

Решение.

а) Решим сравнение

$$x^2 \equiv 207(\mathrm{mod}\,191). \qquad (11)$$

Заметим, что $207 \equiv 16(\mathrm{mod}\,191)$. Поэтому вместо исходного сравнения можно решать сравнение

$$x^2 \equiv 16(\mathrm{mod}\,191). \qquad (12)$$

Тогда $x \equiv 4(\mathrm{mod}\,191)$, $x \equiv -4(\mathrm{mod}\,191)$.

Ответ: $x \equiv 4(\mathrm{mod}\,191)$, $x \equiv -4(\mathrm{mod}\,191)$.

б) Рассмотрим сравнение

$$x^2 \equiv 188 (\mathrm{mod}\, 263). \qquad (13)$$

Модуль сравнения (13) равен 263 и является простым числом. Выясним, имеет ли сравнение (13) решения. Для того чтобы определить, есть ли решения у сравнения, найдем символ Лежандра, используя его свойства (приложение Б):

$$\left(\frac{188}{263}\right) = \left(\frac{2^2 \cdot 47}{263}\right) = \left|свойство\ 3\right| = \left(\frac{47}{263}\right) = \left|свойство\ 7\right| = (-1)^{\frac{47-1}{2}\cdot\frac{263-1}{2}} \left(\frac{263}{47}\right) =$$

$$= |\, свойство\ 1| = -\left(\frac{28}{47}\right) = -\left(\frac{2^2 \cdot 7}{47}\right) = |\, свойство\ 3| = -\left(\frac{7}{47}\right) = |\, свойство\ 7\,| =$$

$$= -(-1)^{\frac{7-1}{2}\cdot\frac{47-1}{2}} \left(\frac{47}{7}\right) = |\, свойство\ 1| = \left(\frac{5}{7}\right) = |\, свойство\ 7\,| = (-1)^{\frac{5-1}{2}\cdot\frac{7-1}{2}} \left(\frac{7}{5}\right) = .$$

$$= |\, свойство\ 1| = \left(\frac{2}{5}\right) = |\, свойство\ 6\,| = -1.$$

Так как символ Лежандра $\left(\frac{188}{263}\right)$ равен -1, то число 188 является невычетом по модулю 263 и сравнение (13) решений не имеет.

Ответ: решений нет.

в) Решим сравнение

$$x^2 \equiv 146 (\mathrm{mod}\, 311). \qquad (14)$$

Модуль сравнения (14) равен 311 и является простым числом. Выясним, имеет ли сравнение (14) решения. Для того чтобы определить, есть ли решения у сравнения, найдем символ Лежандра:

$$\left(\frac{146}{311}\right) = \left(\frac{2 \cdot 73}{311}\right) = |\, свойство\ 3| = \left(\frac{2}{311}\right)\left(\frac{73}{311}\right) = \begin{vmatrix} свойство\ 6, \\ свойство\ 7 \end{vmatrix} =$$

$$= (-1)^{\frac{311^2-1}{8}} \cdot (-1)^{\frac{73-1}{2}\cdot\frac{311-1}{2}} \left(\frac{311}{73}\right) = (-1)^{\frac{310\cdot 312}{8}} \cdot (-1)^{\frac{72}{2}\cdot\frac{310}{2}} \left(\frac{311}{73}\right) = \left(\frac{311}{73}\right) = |\, свойство\ 1| =$$

$$= \left(\frac{19}{73}\right) = |\, свойство\ 7\,| = (-1)^{\frac{19-1}{2}\cdot\frac{73-1}{2}} \left(\frac{73}{19}\right) = \left(\frac{73}{19}\right) = |\, свойство\ 1| = \left(\frac{16}{19}\right) = \left(\frac{2^4}{19}\right) =$$

$$=\left(\frac{2}{19}\right)^4=1.$$

Так как символ Лежандра $\left(\frac{146}{311}\right)$ равен 1, то число 146 является вычетом по модулю 311 и сравнение (14) имеет решения.

Найдем решения сравнения (14).

Модуль сравнения $p=311$ удовлетворяет условию $p\equiv 3(\mathrm{mod}\,4)$, то есть $311\equiv 3(\mathrm{mod}\,4)$. В этом случае для нахождения решений сравнения можно воспользоваться свойством квадратичных вычетов, согласно которому, если a является квадратичным вычетом по простому модулю p, то $a^{\frac{p-1}{2}}\equiv 1(\mathrm{mod}\,p)$. Итак, $146^{\frac{311-1}{2}}\equiv 1(\mathrm{mod}\,311)$ или $146^{155}\equiv 1(\mathrm{mod}\,311)$. Умножим обе части последнего сравнения на 146, получим $146^{156}\equiv 146(\mathrm{mod}\,311)$ или $(146^{78})^2\equiv 146(\mathrm{mod}\,311)$. Тогда одним из решений квадратичного сравнения (14) является $x\equiv 146^{78}(\mathrm{mod}\,311)$.

Найдем $146^{78}(\mathrm{mod}\,311)$. Воспользуемся бинарным (индийским) методом возведения в степень.

Находим представление числа 78 в двоичной системе счисления:

$78_{10}=1001110_2$.

Формируем правило возведения в степень. Заменим каждую цифру «1» на пару букв «SM_{146}» и каждую цифру «0» на букву «S», получим последовательность «$SM_{146}SSSM_{146}SM_{146}SM_{146}S$». Теперь вычеркнем пару букв «SM_{146}» слева. Получившаяся последовательность букв «$SSSM_{146}SM_{146}SM_{146}S$» представляет собой правило для вычисления $146^{78}(\mathrm{mod}\,311)$, если интерпретировать «S» как «возвести в квадрат и взять остаток по модулю 311», а «M_{146}» как «умножить на 146 и взять остаток по модулю 311».

Проводя вычисления последовательно, получим следующие результаты:

$146^2(\mathrm{mod}\,311)\equiv 168(\mathrm{mod}\,311)$,

$$168^2 \pmod{311} \equiv 234 \pmod{311} \equiv -77 \pmod{311},$$

$$(-77)^2 \pmod{311} \equiv 20 \pmod{311},$$

$$20 \cdot 146 \pmod{311} \equiv 121 \pmod{311},$$

$$121^2 \pmod{311} \equiv 24 \pmod{311},$$

$$24 \cdot 146 \pmod{311} \equiv 83 \pmod{311},$$

$$83^2 \pmod{311} \equiv 47 \pmod{311},$$

$$47 \cdot 146 \pmod{311} \equiv 20 \pmod{311},$$

$$20^2 \pmod{311} \equiv 89 \pmod{311}.$$

Итак, $x \equiv 146^{78} \pmod{311} \equiv 89 \pmod{311}$ – одно решение сравнения, $x \equiv (311-89) \pmod{311} \equiv 222 \pmod{311}$ – второе решение сравнения.

Ответ: $x \equiv 89 \pmod{311}$, $x \equiv 222 \pmod{311}$.

г) Решим сравнение

$$x^2 \equiv 34 \pmod{61}. \qquad (15)$$

Модуль сравнения (15) равен 61 и является простым числом. Выясним, имеет ли сравнение (15) решения. Для того чтобы определить, есть ли решения у сравнения, найдем символ Лежандра:

$$\left(\frac{34}{61}\right) = \left(\frac{2 \cdot 17}{61}\right) = |\textit{свойство } 3| = \left(\frac{2}{61}\right)\left(\frac{17}{61}\right) = \begin{vmatrix} \textit{свойство } 6, \\ \textit{свойство } 7 \end{vmatrix} =$$

$$= (-1)^{\frac{61^2-1}{8}} \cdot (-1)^{\frac{17-1}{2}\cdot\frac{61-1}{2}} \left(\frac{61}{17}\right) = -\left(\frac{61}{17}\right) = |\textit{свойство } 1| = -\left(\frac{10}{17}\right) = -\left(\frac{2 \cdot 5}{17}\right) =$$

$$= |\textit{свойство } 3| = -\left(\frac{2}{17}\right)\left(\frac{5}{17}\right) = \begin{vmatrix} \textit{свойство } 6, \\ \textit{свойство } 7 \end{vmatrix} = -(1)^{\frac{5-1}{2}\cdot\frac{17-1}{2}} \left(\frac{17}{5}\right) = -\left(\frac{17}{5}\right) =$$

$$= |\textit{свойство } 1| = -\left(\frac{2}{5}\right) = |\textit{свойство } 6| = -1 \cdot (-1) = 1.$$

Так как символ Лежандра $\left(\frac{34}{61}\right)$ равен 1, то число 34 является вычетом по модулю 61 и сравнение (15) имеет решения.

Найдем решения сравнения (15).

Модуль сравнения $p = 61$ удовлетворяет условию $p \equiv 5(\mathrm{mod}8)$, то есть $61 \equiv 5(\mathrm{mod}8)$. В этом случае для нахождения решений сравнения можно воспользоваться свойством квадратичных вычетов, согласно которому, если a является квадратичным вычетом по простому модулю p, то $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p)$. Итак, $34^{\frac{61-1}{2}} \equiv 1(\mathrm{mod}61)$ или $34^{30} \equiv 1(\mathrm{mod}61)$.

Найдем $34^{15}(\mathrm{mod}61)$. Воспользуемся бинарным (индийским) методом возведения в степень.

Находим представление числа 15 в двоичной системе счисления:

$$15_{10} = 1111_2.$$

Формируем правило возведения в степень. Заменяя каждую цифру «1» на пару букв «SM_{34}», получим последовательность «$SM_{34}SM_{34}SM_{34}SM_{34}$». Теперь вычеркнем пару букв «SM_{34}» слева. Получившаяся последовательность букв «$SM_{34}SM_{34}SM_{34}$» представляет собой правило для вычисления $34^{15}(\mathrm{mod}61)$.

Проводя вычисления последовательно, получим следующие результаты:

$34^2(\mathrm{mod}61) \equiv 58(\mathrm{mod}61) \equiv -3(\mathrm{mod}61)$,

$-3 \cdot 34(\mathrm{mod}61) \equiv 20(\mathrm{mod}61)$,

$20^2(\mathrm{mod}61) \equiv 34(\mathrm{mod}61)$,

$34 \cdot 34(\mathrm{mod}61) \equiv 58(\mathrm{mod}61) \equiv -3(\mathrm{mod}61)$,

$(-3)^2(\mathrm{mod}61) \equiv 9(\mathrm{mod}61)$,

$9 \cdot 34(\mathrm{mod}61) \equiv 1(\mathrm{mod}61)$.

Итак, $34^{15} \equiv 1(\mathrm{mod}61)$. Умножим обе части последнего сравнения на 34. Получим сравнение $34^{16} \equiv 34(\mathrm{mod}61)$ или $(34^8)^2 \equiv 34(\mathrm{mod}61)$. Сравнивая полученное сравнение со сравнением (15) заключаем, что одно из решений сравнения (15) находится как $x \equiv 34^8(\mathrm{mod}61) \equiv 20(\mathrm{mod}61)$. Другое решение сравнения (15) имеет вид $x \equiv (61-20)(\mathrm{mod}61) \equiv 41(\mathrm{mod}61)$.

Ответ: $x \equiv 20(\mathrm{mod}61)$, $x \equiv 41(\mathrm{mod}61)$.

д) Решим сравнение

$$x^2 \equiv 62 (\mathrm{mod} 97). \qquad (16)$$

Модуль сравнения (16) равен 97 и является простым числом. Выясним, имеет ли сравнение (16) решения. Для того чтобы определить, есть ли решения у сравнения, найдем символ Лежандра:

$$\left(\frac{62}{97}\right) = \left(\frac{2 \cdot 31}{97}\right) = |\, свойство\ 3 \,| = \left(\frac{2}{97}\right)\left(\frac{31}{97}\right) = \left| \begin{matrix} свойство\ 6, \\ свойство\ 7 \end{matrix} \right| =$$

$$= (-1)^{\frac{97^2-1}{8}} \cdot (-1)^{\frac{31-1}{2}\cdot\frac{97-1}{2}} \left(\frac{97}{31}\right) = \left(\frac{97}{31}\right) = |\, свойство\ 1 \,| = \left(\frac{4}{31}\right) = \left(\frac{2^2}{31}\right) = \left(\frac{2}{31}\right)^2 = 1.$$

Так как символ Лежандра $\left(\frac{62}{97}\right)$ равен 1, то число 62 является вычетом по модулю 97 и сравнение (16) имеет решения.

Буем искать решения сравнения (16), используя алгоритм Шенкса.

Напомним последовательность действий алгоритма Шенкса решения сравнения $x^2 \equiv a (\mathrm{mod}\, p)$, где p является простым числом, a – квадратичным вычетом по модулю p:

1) выбрать n такое, что $\left(\frac{n}{p}\right) = -1$;

2) найти целые числа e, q, удовлетворяющие соотношению $p - 1 = 2^e q$, где q – нечетное;

3) положить $y \equiv n^q (\mathrm{mod}\, p)$, $r = e$, $x \equiv a^{\frac{q-1}{2}} (\mathrm{mod}\, p)$;

4) положить $b \equiv ax^2 (\mathrm{mod}\, p)$, $x \equiv ax (\mathrm{mod}\, p)$;

5) выполнить цикл. Пока $b \neq 1 (\mathrm{mod}\, p)$ делать:

а) найти наименьшее m, такое, что $b^{2^m} \equiv 1 (\mathrm{mod}\, p)$;

б) положить $t \equiv y^{2^{r-m-1}} (\mathrm{mod}\, p)$, $y \equiv t^2 (\mathrm{mod}\, p)$, $r = m$;

в) $x \equiv xt (\mathrm{mod}\, p)$, $b \equiv by (\mathrm{mod}\, p)$;

6) найденное значение x будет одним из решений сравнения $x^2 \equiv a(\mathrm{mod}\, p)$. Второе решения находится как $p - x$.

Запишем алгоритм Шенкса для сравнения (16):

1) при $n = 5$ символ Лежанда $\left(\frac{5}{97}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{97-1}{2}}\left(\frac{97}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1$;

2) $p - 1 = 97 - 1 = 96 = 2^5 \cdot 3$, то есть $e = 5$, $q = 3$;

3) положим $y \equiv 5^3(\mathrm{mod}97) \equiv 28(\mathrm{mod}97)$, $r = 5$,

$x \equiv 62^{\frac{3-1}{2}}(\mathrm{mod}97) \equiv 62(\mathrm{mod}97) \equiv -35(\mathrm{mod}97)$;

4) положим $b \equiv 62 \cdot 62^2(\mathrm{mod}97) \equiv -35 \cdot (-35)^2(\mathrm{mod}97) \equiv 96(\mathrm{mod}97) \equiv -1(\mathrm{mod}97)$,

$x \equiv 62 \cdot 62(\mathrm{mod}97) \equiv (-35) \cdot (-35)(\mathrm{mod}97) \equiv 61(\mathrm{mod}97) \equiv -36(\mathrm{mod}97)$;

5) выполним цикл. Пока $b \neq 1(\mathrm{mod}97)$ делаем:

I $b \equiv -1(\mathrm{mod}97)$;

а) наименьшее m, такое, что $(-1)^{2^m} \equiv 1(\mathrm{mod}97)$, равно 1;

б) положим $t \equiv 28^{2^{5-1-1}}(\mathrm{mod}97) \equiv 28^8(\mathrm{mod}97) \equiv 22(\mathrm{mod}97)$,

$y \equiv 22^2(\mathrm{mod}97) \equiv 96(\mathrm{mod}97) \equiv -1(\mathrm{mod}97)$, $r = 1$;

в) $x \equiv -36 \cdot 22(\mathrm{mod}97) \equiv -36 \cdot 22(\mathrm{mod}97) \equiv 81(\mathrm{mod}97)$,

$b \equiv -1 \cdot (-1)(\mathrm{mod}97) \equiv 1(\mathrm{mod}97)$;

$b \equiv 1(\mathrm{mod}97)$ поэтому цикл завершен;

6) найденное значение $x \equiv 81(\mathrm{mod}97)$ будет одним из решений сравнения (16). Второе решение находится как $x \equiv (97 - 81)(\mathrm{mod}97) \equiv 16(\mathrm{mod}97)$.

Ответ: $x \equiv 81(\mathrm{mod}97)$, $x \equiv 16(\mathrm{mod}97)$.

е) Решим сравнение

$$x^2 \equiv 145(\mathrm{mod}51). \qquad (17)$$

Заметим, что $145 \equiv 43(\mathrm{mod}51)$. Поэтому вместо исходного сравнения можно решать сравнение

$$x^2 \equiv 43(\mathrm{mod}51). \qquad (18)$$

Модуль сравнения (18) равен 51 и является составным числом, каноническое разложение которого имеет вид $51=3\cdot17$, то есть является произведением первых степеней простых чисел. В этом случае решение сравнения сводится к нахождению решения систем сравнений. Из того, что $x^2\equiv43(\mathrm{mod}51)$ следует, что $x^2\equiv43(\mathrm{mod}3)$ и $x^2\equiv43(\mathrm{mod}17)$. Так как $43\equiv1(\mathrm{mod}3)$, $43\equiv9(\mathrm{mod}17)$, то получим следующую систему квадратичных сравнений:

$$\begin{cases} x^2\equiv1(\mathrm{mod}3), \\ x^2\equiv9(\mathrm{mod}17). \end{cases} \tag{19}$$

Первое сравнение системы (19) имеет два решения:

$$x\equiv1(\mathrm{mod}3) \text{ и } x\equiv-1(\mathrm{mod}3).$$

Второе сравнение системы (19) также имеет два решения:

$$x\equiv3(\mathrm{mod}17) \text{ и } x\equiv-3(\mathrm{mod}17).$$

Выбирая из каждой пары решения по одному корню, составим следующую совокупность систем линейных сравнений:

$$\left[\begin{array}{l} \begin{cases} x\equiv1(\mathrm{mod}3), \\ x\equiv3(\mathrm{mod}17), \end{cases} \\ \begin{cases} x\equiv-1(\mathrm{mod}3), \\ x\equiv3(\mathrm{mod}17), \end{cases} \\ \begin{cases} x\equiv1(\mathrm{mod}3), \\ x\equiv-3(\mathrm{mod}17), \end{cases} \\ \begin{cases} x\equiv-1(\mathrm{mod}3), \\ x\equiv-3(\mathrm{mod}17), \end{cases} \end{array}\right. \tag{20}$$

Решим первую систему совокупности (20):

$$\begin{cases} x\equiv1(\mathrm{mod}3), \\ x\equiv3(\mathrm{mod}17). \end{cases} \tag{21}$$

Так как *НОД*(3,7) = 1, то система (21) имеет единственное решение.

Из первого сравнения системы (21) $x\equiv1(\mathrm{mod}3)$ следует, что $x=1+3k,\ k\in Z$. Чтобы найти k, подставим x во второе сравнение: $1+3k\equiv3(\mathrm{mod}17)$ или $3k\equiv2(\mathrm{mod}17)$. Так как $2\equiv-15(\mathrm{mod}17)$, то $3k\equiv-15(\mathrm{mod}17)$. Разделим обе части

последнего сравнения на 3, получим сравнение $k \equiv -5(\mathrm{mod}17) \equiv 12(\mathrm{mod}17)$ или $k = 12 + 17t,\ t \in Z$. Следовательно, решением системы сравнений (21) является $x = 1 + 3(12 + 17t) = 37 + 51t,\ t \in Z$, то есть $x \equiv 37(\mathrm{mod}51)$. Это же решение является первым решением квадратичного сравнения (17).

Решим вторую систему совокупности (20):

$$\begin{cases} x \equiv -1(\mathrm{mod}3), \\ x \equiv 3(\mathrm{mod}17). \end{cases} \qquad (22)$$

Так как *НОД*(3,7) = 1, то система (22) имеет единственное решение.

Из первого сравнения системы (22) $x \equiv -1(\mathrm{mod}3) \equiv 2(\mathrm{mod}3)$ следует, что $x = 2 + 3k,\ k \in Z$. Чтобы найти *k*, подставим *x* во второе сравнение: $2 + 3k \equiv 3(\mathrm{mod}17)$ или $3k \equiv 1(\mathrm{mod}17)$. Так как $3^{-1}(\mathrm{mod}17) = 6$, то $k \equiv 3^{-1}(\mathrm{mod}17) \equiv 6(\mathrm{mod}17)$ или $k = 6 + 17t,\ t \in Z$. Следовательно, решением системы сравнений (22) является $x = 2 + 3(6 + 17t) = 20 + 51t,\ t \in Z$, то есть $x \equiv 20(\mathrm{mod}51)$. Получили второе решение квадратичного сравнения (17).

Решим третью систему совокупности (20):

$$\begin{cases} x \equiv 1(\mathrm{mod}3), \\ x \equiv -3(\mathrm{mod}17). \end{cases} \qquad (23)$$

Так как *НОД*(3,7) = 1, то система (23) имеет единственное решение.

Из первого савнения системы (23) $x \equiv 1(\mathrm{mod}3)$ следует, что $x = 1 + 3k,\ k \in Z$. Чтобы найти *k*, подставим *x* во второе сравнение: $1 + 3k \equiv -3(\mathrm{mod}17)$ или $3k \equiv -4(\mathrm{mod}17)$. Так как $3^{-1}(\mathrm{mod}17) = 6$, то $k \equiv -4 \cdot 3^{-1}(\mathrm{mod}17) \equiv -4 \cdot 6(\mathrm{mod}17) \equiv$ $\equiv 10(\mathrm{mod}17)$ или $k = 10 + 17t,\ t \in Z$. Следовательно, решением системы сравнений (23) является $x = 1 + 3(10 + 17t) = 31 + 51t,\ t \in Z$, то есть $x \equiv 31(\mathrm{mod}51)$. Получили третье решение квадратичного сравнения (17).

Решим четвертую систему совокупности (20):

$$\begin{cases} x \equiv -1(\mathrm{mod}3), \\ x \equiv -3(\mathrm{mod}17). \end{cases} \qquad (24)$$

Так как *НОД*(3,7) = 1, то система (24) имеет единственное решение.

Из первого сравнения системы (24) $x \equiv -1(\mathrm{mod}\,3) \equiv 2(\mathrm{mod}\,3)$ следует, что $x = 2 + 3k,\ k \in Z$. Чтобы найти k, подставим x во второе сравнение: $2 + 3k \equiv -3(\mathrm{mod}17)$ или $3k \equiv -5(\mathrm{mod}17)$. Так как $-5 \equiv 12(\mathrm{mod}17)$, то $3k \equiv 12(\mathrm{mod}17)$. Разделим обе части последнего сравнения на 3, получим сравнение $k \equiv 4(\mathrm{mod}17)$ или $k = 4 + 17t,\ t \in Z$. Следовательно, решением системы сравнений (24) является $x = 2 + 3(4 + 17t) = 14 + 51t,\ t \in Z$, то есть $x \equiv 14(\mathrm{mod}\,51)$. Это же решение является четвертым решением квадратичного сравнения (17).

Ответ: $x \equiv 14(\mathrm{mod}\,51)$, $x \equiv 20(\mathrm{mod}\,51)$, $x \equiv 31(\mathrm{mod}\,51)$, $x \equiv 37(\mathrm{mod}\,51)$.

Задание 5. Найти первообразный корень по модулю m:

а) $m = 229$; б) $m = 6859$; в) $m = 1250$.

Решение.

а) Найдем первообразный корень по модулю $m = 229$.

Напомним, что число *a* называется первообразным корнем по модулю *m*, где *НОД*(*a*,*m*) = 1, если показатель по этому модулю равен значению функции Эйлера, то есть $P_m(a) = \varphi(m)$.

Модуль $m = 229$ является простым числом. Согласно теореме о существовании первообразных корней, первообразный корень по простому числу существует. Чтобы его найти, воспользуемся утверждением, согласно которому если $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ – каноническое разложение числа $\varphi(p) = p - 1$, где p – простое число, и

$$a^{\frac{p-1}{p_1}} \neq 1(\mathrm{mod}\ p), \ldots, a^{\frac{p-1}{p_s}} \neq 1(\mathrm{mod}\ p), \qquad (25)$$

то *a* является первообразным корнем по простому модулю *p*.

Найдем каноническое разложение числа $m - 1 = 228 = 2^2 \cdot 3 \cdot 19$. Выберем любое число *a*, взаимно простое с числом $m = 229$, например, $a = 6$, и выясним, является ли оно первообразным корнем по модулю 229. Для этого необходимо проверить выполнение условий (25):

$$6^{\frac{228}{2}} \neq 1(\mathrm{mod}\,229),\ 6^{\frac{228}{3}} \neq 1(\mathrm{mod}\,229) \text{ и } 6^{\frac{228}{19}} \neq 1(\mathrm{mod}\,229).$$

Находим $6^{\frac{228}{2}} (\mathrm{mod}\, 229) = 6^{114} (\mathrm{mod}\, 229)$. Правило возведения в степень имеет вид «$SM_6SM_6SSSM_6S$». Проводя вычисления последовательно, получим:

$6^2 (\mathrm{mod}\, 229) = 36,$

$36 \cdot 6 (\mathrm{mod}\, 229) \equiv 216 (\mathrm{mod}\, 229) \equiv -13 (\mathrm{mod}\, 229),$

$(-13)^2 (\mathrm{mod}\, 229) \equiv 169 (\mathrm{mod}\, 229) \equiv -60 (\mathrm{mod}\, 229),$

$-60 \cdot 6 (\mathrm{mod}\, 229) \equiv 98 (\mathrm{mod}\, 229),$

$98^2 (\mathrm{mod}\, 229) \equiv 215 (\mathrm{mod}\, 229) \equiv -14 (\mathrm{mod}\, 229),$

$(-14)^2 (\mathrm{mod}\, 229) \equiv 196 (\mathrm{mod}\, 229) \equiv -33 (\mathrm{mod}\, 229),$

$(-33)^2 (\mathrm{mod}\, 229) \equiv 173 (\mathrm{mod}\, 229) \equiv -56 (\mathrm{mod}\, 229),$

$-56 \cdot 6 (\mathrm{mod}\, 229) \equiv -107 (\mathrm{mod}\, 229),$

$(-107)^2 (\mathrm{mod}\, 229) \equiv 228 (\mathrm{mod}\, 229) \equiv -1 (\mathrm{mod}\, 229).$

Итак, $6^{\frac{228}{2}} \neq 1 (\mathrm{mod}\, 229)$. Переходим к проверке следующего условия.

Найдем $6^{\frac{228}{3}} (\mathrm{mod}\, 229) = 6^{76} (\mathrm{mod}\, 229)$. Правило возведения в степень имеет вид «$SSSM_6SM_6SS$». Проводя вычисления последовательно, получим:

$6^2 (\mathrm{mod}\, 229) = 36,$

$36^2 (\mathrm{mod}\, 229) \equiv 151 (\mathrm{mod}\, 229) \equiv -78 (\mathrm{mod}\, 229),$

$(-78)^2 (\mathrm{mod}\, 229) \equiv 130 (\mathrm{mod}\, 229) \equiv -99 (\mathrm{mod}\, 229),$

$-99 \cdot 6 (\mathrm{mod}\, 229) \equiv 93 (\mathrm{mod}\, 229),$

$93^2 (\mathrm{mod}\, 229) \equiv 176 (\mathrm{mod}\, 229) \equiv -53 (\mathrm{mod}\, 229),$

$-53 \cdot 6 (\mathrm{mod}\, 229) \equiv -89 (\mathrm{mod}\, 229),$

$(-89)^2 (\mathrm{mod}\, 229) \equiv 135 (\mathrm{mod}\, 229) \equiv -94 (\mathrm{mod}\, 229),$

$(-94)^2 (\mathrm{mod}\, 229) \equiv 134 (\mathrm{mod}\, 229).$

Итак, $6^{\frac{228}{3}} \neq 1 (\mathrm{mod}\, 229)$. Переходим к проверке следующего условия.

Найдем $6^{\frac{228}{19}} (\mathrm{mod}\, 229) = 6^{12} (\mathrm{mod}\, 229)$. Правило возведения в степень имеет вид «SM_6SS». Проводя вычисления последовательно, получим:

$6^2 (\mathrm{mod}\, 229) = 36,$

$36 \cdot 6 (\mathrm{mod}\, 229) \equiv 216 (\mathrm{mod}\, 229) \equiv -13 (\mathrm{mod}\, 229),$

$(-13)^2 (\mathrm{mod}\, 229) \equiv 169 (\mathrm{mod}\, 229) \equiv -60 (\mathrm{mod}\, 229),$

$(-60)^2 (\mathrm{mod}\, 229) \equiv 165 (\mathrm{mod}\, 229).$

Итак, $6^{\frac{228}{19}} \neq 1 (\mathrm{mod}\, 229)$.

Таки образом, 6 является первообразным корнем по модулю 229.

Ответ: 6.

б) Найдем первообразный корень по модулю $m = 6859$.

Так как модуль $m = 6859$ является степенью простого числа, то есть $6859 = 19^3$, то первообразный корень по данному модулю существует. Чтобы его найти, воспользуемся утверждением, согласно которому, если a – первообразный корень по простому модулю p и

$$a^{p^{\alpha-2}(p-1)} \neq 1 (\mathrm{mod}\, p^{\alpha}), \text{ где } \alpha \geq 2, \qquad (26)$$

то a является также первообразным корнем по модулю p^{α}.

Сначала необходимо найти первообразный корень по простому модулю $p = 19$. Каноническое разложение числа $p - 1 = 18 = 2 \cdot 3^2$. Выберем любое число a, взаимно простое с числом $p = 19$, например, $a = 3$, и выясним, является ли оно первообразным корнем по модулю 19. Для этого необходимо проверить выполнение следующих условий:

$$3^{\frac{18}{2}} \neq 1 (\mathrm{mod} 19) \text{ и } 3^{\frac{18}{3}} \neq 1 (\mathrm{mod} 19).$$

Находим $3^{\frac{18}{2}} (\mathrm{mod} 19) = 3^9 (\mathrm{mod} 19) \equiv 18 (\mathrm{mod} 19) \neq 1 (\mathrm{mod} 19);$

$3^{\frac{18}{2}} (\mathrm{mod} 19) = 3^9 (\mathrm{mod} 19) \equiv 18 (\mathrm{mod} 19) \neq 1 (\mathrm{mod} 19).$

Итак, $a = 3$ является первообразным корнем по модулю 19.

Для найденного первообразного корня проверим условие (26), в котором $a=3,\ \alpha=3,\ p=19$.

Вычислим $3^{19^{3-2}(19-1)}(\mathrm{mod}19^3)=3^{342}(\mathrm{mod}6859)$. Правило возведения в степень имеет вид «$SSM_3SSM_3SSM_3SM_3S$». Проводя вычисления последовательно, получим:

$3^2(\mathrm{mod}6859)=9,$

$9^2(\mathrm{mod}6859)=81,$

$81\cdot 3(\mathrm{mod}6859)=243,$

$243^2(\mathrm{mod}6859)\equiv 4177(\mathrm{mod}6859)\equiv -2682(\mathrm{mod}6859),$

$(-2682)^2(\mathrm{mod}6859)\equiv 4892(\mathrm{mod}6859)\equiv -1967(\mathrm{mod}6859),$

$-1967\cdot 3(\mathrm{mod}6859)\equiv 958(\mathrm{mod}6859),$

$958^2(\mathrm{mod}6859)\equiv 5517(\mathrm{mod}6859)\equiv -1342(\mathrm{mod}6859),$

$(-1342)^2(\mathrm{mod}6859)\equiv 3906(\mathrm{mod}6859),$

$3906\cdot 3(\mathrm{mod}6859)\equiv 4859(\mathrm{mod}6859)\equiv -2000(\mathrm{mod}6859),$

$(-2000)^2(\mathrm{mod}6859)\equiv 1203(\mathrm{mod}6859),$

$1203\cdot 3(\mathrm{mod}6859)\equiv 3609(\mathrm{mod}6859),$

$3609^2(\mathrm{mod}6859)\equiv 6499(\mathrm{mod}6859).$

Итак, $3^{19^{3-2}(19-1)}(\mathrm{mod}19^3)\equiv 6499(\mathrm{mod}6859)\neq 1(\mathrm{mod}6859)$.

Таким образом, 3 является первообразным корнем по модулю 6859.

Ответ: 3.

в) Найдем первообразный корень по модулю $m=1250$.

Так как модуль $m=1250=2\cdot 5^4$, то есть имеет вид $2\cdot p^\alpha$, где p – простое число, $\alpha\geq 1$ – целое, то первообразный корень по данному модулю существует. Чтобы его найти, воспользуемся утверждением, согласно которому любой нечетный первообразный корень по модулю p^α, где p – простое число, $\alpha\geq 1$ – целое, также является первообразным корнем по модулю $2\cdot p^\alpha$.

Сначала необходимо найти первообразный корень по простому модулю $p=5$.

Для этого воспользуемся определением первообразного корня. Выберем нечетное число $a=3$. Так как $\varphi(5)=4$, то найдем $3^2(\mathrm{mod}\,5)=4\neq 1(\mathrm{mod}\,5)$, $3^4(\mathrm{mod}\,5)\equiv 1(\mathrm{mod}\,5)$. Таким образом, $P_5(3)=4=\varphi(5)$ и 3 является первообразным корнем по модулю 5.

Выясним, является ли $a=3$ первообразным корнем по модулю 5^4. Для этого проверим условие (26), в котором $a=3$, $\alpha=4$, $p=5$. Вычислим $3^{5^{4-2}(4-1)}(\mathrm{mod}\,5^4)=3^{75}(\mathrm{mod}\,625)$. Правило возведения в степень имеет вид «$SSSM_3SSM_3SM_3$». Проводя вычисления последовательно, получим:

$3^2(\mathrm{mod}\,625)=9,$

$9^2(\mathrm{mod}\,625)=81,$

$81^2(\mathrm{mod}\,625)\equiv 311(\mathrm{mod}\,625),$

$311\cdot 3(\mathrm{mod}\,625)\equiv 308(\mathrm{mod}\,625),$

$308^2(\mathrm{mod}\,625)\equiv 489(\mathrm{mod}\,625)\equiv -136(\mathrm{mod}\,625),$

$(-136)^2(\mathrm{mod}\,625)\equiv 371(\mathrm{mod}\,625),$

$371\cdot 3(\mathrm{mod}\,625)\equiv 488(\mathrm{mod}\,625)\equiv -137(\mathrm{mod}\,625),$

$(-137)^2(\mathrm{mod}\,625)\equiv 19(\mathrm{mod}\,625),$

$19\cdot 3(\mathrm{mod}\,625)\equiv 57(\mathrm{mod}\,625).$

Итак, $3^{5^{4-2}(4-1)}(\mathrm{mod}\,5^4)=3^{75}(\mathrm{mod}\,625)\neq 1(\mathrm{mod}\,625)$.

Таким образом, 3 является первообразным корнем по модулю 5^4.

Так как 3 – нечетный первообразный корень по модулю 5^4, то он также является первообразным корнем по модулю $2\cdot 5^4=1250$.

Ответ: 3.

Задание 6. Составить таблицу индексов по модулю 13. Используя данную таблицу, решить сравнения:

а) $7x\equiv 9(\mathrm{mod}13)$; б) $x^3\equiv 12(\mathrm{mod}13)$.

Решение.

Составим таблицу индексов по модулю 13. Число 2 является первообразным корнем по модулю 13, так как $2^{12} \equiv 1(\text{mod}13)$, но $2^6 \neq 1(\text{mod}13)$, $2^4 \neq 1(\text{mod}13)$. Тогда числа $2^0, 2^1, 2^2, ..., 2^{11}$ образуют приведенную систему вычетов по модулю 13, то есть $2^0 \equiv 1(\text{mod}13)$, $2^1 \equiv 2(\text{mod}13)$, $2^2 \equiv 4(\text{mod}13)$, $2^3 \equiv 8(\text{mod}13)$, $2^4 \equiv 3(\text{mod}13)$, $2^5 \equiv 6(\text{mod}13)$, $2^6 \equiv 12(\text{mod}13)$, $2^7 \equiv 11(\text{mod}13)$, $2^8 \equiv 9(\text{mod}13)$, $2^9 \equiv 5(\text{mod}13)$, $2^{10} \equiv 10(\text{mod}13)$, $2^{11} \equiv 7(\text{mod}13)$. Таким образом, $ind1 = 0$, $ind2 = 1$, $ind3 = 4$, $ind4 = 2$, $ind5 = 9$, $ind6 = 5$, $ind7 = 11$, $ind8 = 3$, $ind9 = 8$, $ind10 = 10$, $ind11 = 7$, $ind12 = 6$. Оформим найденные индексы по модулю 13 в виде таблицы 3.

Таблица 3 – Таблица индексов по модулю 13

a	1	2	3	4	5	6	7	8	9	10	11	12
$inda$	0	1	4	2	9	5	11	3	8	10	7	6

а) Решим сравнение

$$7x \equiv 9(\text{mod}13). \qquad (27)$$

Так как $НОД(7,13) = 1$, то сравнение (27) имеет решения, причем в кольце Z_{13} решение единственно.

Пользуясь свойствами индексов, получим $7x \equiv 9(\text{mod}13) \Leftrightarrow$

$\Leftrightarrow ind(7x) \equiv ind9(\text{mod}\,\varphi(13)) \Leftrightarrow ind7 + indx \equiv ind9(\text{mod}12)$.

По таблице 3 находим, что $ind7 = 11$, $ind9 = 8$. Отсюда получаем сравнение $11 + indx \equiv 8(\text{mod}12) \Leftrightarrow indx \equiv 9(\text{mod}12) \Leftrightarrow x \equiv 5(\text{mod}13)$.

Ответ: $x \equiv 5(\text{mod}13)$.

б) Решим сравнение

$$x^3 \equiv 12(\text{mod}13). \qquad (28)$$

Напомним, что если $НОД(a, p) = 1$ и $НОД(n, p-1) = \delta$ для сравнения $x^n \equiv a(\text{mod}\,p)$, где p – простое нечетное число, то сравнение имеет δ решений по

модулю p, если δ делит $ind\,a$, и сравнение не имеет решений, если δ не делит $ind\,a$.

Для сравнения (28) $a=12$, $p=13$, $n=3$. $НОД(a,p)=НОД(12,13)=1$, $НОД(n,p-1)=НОД(3,12)=3$, то есть $\delta=3$. По таблице 3 находим, что $ind\,12=6$. Так как 3 делит 6, то сравнение (28) имеет 3 решения по модулю 13. Пользуясь свойствами индексов, получаем $x^3\equiv 12(\mathrm{mod}13)\Leftrightarrow ind x^3\equiv ind\,12(\mathrm{mod}\,\varphi(13))\Leftrightarrow$ $\Leftrightarrow 3indx\equiv 6(\mathrm{mod}12)$. Разделим обе части сравнения и его модуль на 3. Получим сравнение

$$indx\equiv 2(\mathrm{mod}\,4)\Leftrightarrow\begin{bmatrix} indx\equiv 2(\mathrm{mod}12),\\ indx\equiv 6(\mathrm{mod}12),\\ indx\equiv 10(\mathrm{mod}12)\end{bmatrix}\Leftrightarrow\begin{bmatrix} x\equiv 4(\mathrm{mod}13),\\ x\equiv 12(\mathrm{mod}13),\\ x\equiv 10(\mathrm{mod}13).\end{bmatrix}$$

Ответ: $x\equiv 4(\mathrm{mod}13)$, $x\equiv 10(\mathrm{mod}13)$, $x\equiv 12(\mathrm{mod}13)$.

Задание 7. Известен модуль $n=34189$ и шифрующая экспонента $e=29$ алгоритма *RSA*. Зашифровать букву «О» русского алфавита, при условии, что рассматривается алфавит из 33 букв, нумерация букв алфавите начинается с 1.

Решение.

Номер буквы «О» русского алфавита равен 15. Согласно алгоритму шифрования *RSA*, зашифруем номер буквы «О» следующим образом: $15^{29}(\mathrm{mod}34189)$.

Воспользуемся бинарным алгоритмом возведения в степень.

Сначала представляем число 29 в двоичной системе счисления $29_{10}=11101_2$. Затем формируем правило возведения в степень. Заменим каждую цифру «1» на пару букв «SM_{15}» и каждую цифру «0» на букву «S», получим последовательность «$SM_{15}SM_{15}SM_{15}SSM_{15}$». Теперь вычеркнем пару букв «SM_{15}» слева. Получили последовательность букв «$SM_{15}SM_{15}SSM_{15}$», которая представляет собой правило для вычисления $15^{29}(\mathrm{mod}34189)$. Проводя вычисления последовательно, получим следующие результаты:

$15^2(\mathrm{mod}34189)\equiv 225(\mathrm{mod}34189)$,

$225 \cdot 15 (\mathrm{mod}\, 34189) \equiv 3375 (\mathrm{mod}\, 34189)$,

$3375^2 (\mathrm{mod}\, 34189) \equiv 5688 (\mathrm{mod}\, 34189)$,

$5688 \cdot 15 (\mathrm{mod}\, 34189) \equiv 16942 (\mathrm{mod}\, 34189)$,

$16942^2 (\mathrm{mod}\, 34189) \equiv 14709 (\mathrm{mod}\, 34189)$,

$14709^2 (\mathrm{mod}\, 34189) \equiv 6689 (\mathrm{mod}\, 34189)$,

$6689 \cdot 15 (\mathrm{mod}\, 34189) \equiv 31957 (\mathrm{mod}\, 34189)$.

Итак, зашифрованный номер буквы «О» равен 31957.

Ответ: 31957.

Задание 8. Найти секретный ключ *d* алгоритма *RSA*, если известен модуль $n = 25511$ и открытый ключ $e = 37$.

Решение.

Закрытый ключ *d* можно найти, решив сравнение $ed \equiv 1 (\mathrm{mod}\, \varphi(n))$.

Для нахождения функции Эйлера $\varphi(n)$ нам необходимо знать разложение числа *n* на простые множители. Найдем разложение модуля алгоритма $n = 25511$ на простые множители: $25511 = 97 \cdot 263$. Тогда функция Эйлера $\varphi(n) = \varphi(25511) = \varphi(97 \cdot 263) = \varphi(97) \cdot \varphi(263) = 96 \cdot 262 = 25152$.

Получаем сравнение

$$37d \equiv 1 (\mathrm{mod}\, 25152). \qquad (29)$$

Сравнение (29) имеет решения, так как $НОД(25152, 37) = 1$ (37 – простое число). Следовательно, $d \equiv 37^{-1} (\mathrm{mod}\, 25152)$.

Для нахождения $37^{-1} (\mathrm{mod}\, 25152)$ воспользуемся расширенным алгоритмом Евклида, вычисления согласно которому представлены в таблице 4.

Так как $НОД(25152, 37) = 1 = (-14) \cdot 25152 + 9517 \cdot 37$, то $37^{-1} (\mathrm{mod}\, 25152) = 9517$, а решение сравнения (29) имеет вид $d \equiv 9517 (\mathrm{mod}\, 25152)$.

Итак, закрытый ключ $d \equiv 9517$.

Таблица 4 – Поиск *НОД*(25152,37) и его линейного представления.

i	a_i	x_i	y_i	q_i
0	25152	1	0	-
1	37	0	1	679
2	29	1	–679	1
3	8	–1	680	3
4	5	4	–2719	1
5	3	–5	3399	1
6	2	9	–6118	1
7	1	–14	9517	2
8	0			

Ответ: 9517.

Задание 9. Проверить подлинность сообщения $m = 628$ с цифровой подписью $s = 5895$ от отправителя, шифрующая экспонента которого $e = 37$, а модуль алгоритма *RSA* $n = 7313$.

Решение.

Вычислим прообраз сообщения из подписи:

$m' = s^e (\mathrm{mod}\, n) = 5895^{11} (\mathrm{mod}\, 7313) = 628.$

Так как прообраз сообщения m' равен сообщению m, то подпись верна и сообщение подлинно.

Ответ: сообщение подлинно.

Задание 10. Решить задачу о безопасном хранении ключа, если $K = 7$ – ключ, и любые три человека из четверых, получивших информацию о ключе, могли бы вместе восстановить ключ, но никакая группа людей из двух и менее человек не смогли бы этого сделать. Показать процедуру восстановления ключа по первой, второй и четвертой частям ключа.

Решение.

Напомним алгоритм разделения ключа. Если K – ключ, который необходимо сохранить, и требуется, чтобы любые L человек из тех N ($N > L$), которые получили информацию о ключе, могли бы вместе восстановить ключ, но ни одна группа из $L-1$ человека или менее не могла этого сделать, необходимо выполнить следующие действия:

1) выбрать множество целых чисел $\{p, d_1, d_2, ..., d_N\}$ такое, что

а) $p > K$;

б) $d_1 < d_2 < ... < d_N$;

в) числа $p, d_1, d_2, ..., d_k$ попарно взаимно просты;

г) $d_1 \cdot d_2 \cdot ... \cdot d_L > p \cdot d_{N-L+2} \cdot d_{N-L+3} \cdot ... \cdot d_N$ (произведение L наименьших чисел d_i больше, чем произведение p и $L-1$ наибольших чисел d_i);

2) положить $D = d_1 \cdot d_2 \cdot ... \cdot d_L$. Тогда $\frac{D}{p}$ больше, чем произведение любых $(L-1)$ чисел d_i;

3) выбрать целое число $r \in \left[0, \left[\frac{D}{p} - 1\right]\right]$ так, чтобы число $K' = K + r \cdot p$ попало в интервал $\left[\left[\frac{D}{p}\right], D-1\right]$;

4) между разными людьми распределить числа $K_i \equiv K' (\mathrm{mod}\, d_i)$, $i = 1, 2, ..., N$.

Для нашей задачи $K = 7$, $L = 3$, $N = 4$.

Выберем множество целых чисел $\{p, d_1, d_2, d_3, d_4\}$ такое, что

1) $p > K$;

2) $d_1 < d_2 < d_3 < d_4$;

3) числа p, d_1, d_2, d_3, d_4 попарно взаимно просты;

4) $d_1 \cdot d_2 \cdot d_3 > p \cdot d_3 \cdot d_4$ (произведение трех наименьших чисел больше, чем произведение p и двух наибольших чисел).

Пусть $p=11,\ d_1=19,\ d_2=23,\ d_3=29,\ d_4=31.$

Выполнение первых трех условий очевидно. Проверяем четвертое условие:

$$D=d_1\cdot d_2\cdot d_3=19\cdot 23\cdot 29=12673>9889=11\cdot 29\cdot 31=p\cdot d_3\cdot d_4.$$

Найдем $\left[\frac{D}{p}\right]=\left[\frac{12673}{11}\right]=\left[1152\frac{1}{11}\right]=1152,$

$$\left[\frac{D}{p}-1\right]=\left[\frac{12673}{11}-1\right]=\left[\frac{12662}{11}\right]=\left[1151\frac{1}{11}\right]=1151.$$

Выбираем целое число $r\in[0,1151]$ так, чтобы $K'=7+r\cdot 11\in[1152,12673]$. Возьмем $r=105$, тогда $K'=7+105\cdot 11=1162$.

Находим распределяемые числа следующим образом: $K_i\equiv K'(\mathrm{mod}\,d_i)$, $i=1,2,3,4$.

$$K_1\equiv 1162(\mathrm{mod}19)\ \Rightarrow\ K_1=3;$$

$$K_2\equiv 1162(\mathrm{mod}\,23)\ \Rightarrow\ K_2=12;$$

$$K_3\equiv 1162(\mathrm{mod}\,29)\ \Rightarrow\ K_3=2;$$

$$K_4\equiv 1162(\mathrm{mod}31)\Rightarrow K_4=15.$$

Итак, пары (3,19), (12,23), (2,29), (15,31) являются частями ключа *K*.

Показать процедуру восстановления ключа по первой, второй и четвертой частям ключа, то есть по парам (3,19), (12,23) и (15,31).

Находим K' из следующей системы сравнений:

$$\begin{cases} K'\equiv 3(\mathrm{mod}19), \\ K'\equiv 12(\mathrm{mod}\,23), \\ K'\equiv 15(\mathrm{mod}31). \end{cases} \qquad (30)$$

Модули системы (30) являются взаимно простыми числами. Тогда согласно греко-китайской теореме об остатках система (30) имеет единственное решение в кольце Z_{13547}. Найдем это решение.

Первое сравнение $K'\equiv 3(\mathrm{mod}19)$ справедливо для любого K' вида $K'=3+19q,\ q\in Z$.

Подставляем выражение для K' во второе сравнение. Получаем $3+19q \equiv 12(\mathrm{mod}\,23)$ или $19q \equiv 9(\mathrm{mod}\,23)$. Отсюда $q \equiv 9 \cdot 19^{-1}(\mathrm{mod}\,23)$.

Найдем $19^{-1}(\mathrm{mod}\,23)$. Воспользуемся малой теоремой Ферма, согласно которой $19^{22} \equiv 1(\mathrm{mod}\,23)$. Тогда $19 \cdot 19^{21} \equiv 1(\mathrm{mod}\,23)$ и, следовательно, $19^{-1}(\mathrm{mod}\,23) \equiv 19^{21}(\mathrm{mod}\,23)$. Правило возведения в степень имеет вид «$SSM_{19}SSM_{19}$». Проводя вычисления последовательно, получим:

$19^2(\mathrm{mod}\,23) \equiv (-4)^2(\mathrm{mod}\,23) \equiv 16(\mathrm{mod}\,23) \equiv -7(\mathrm{mod}\,23)$,

$(-7)^2(\mathrm{mod}\,23) \equiv 3(\mathrm{mod}\,23)$,

$3 \cdot 19(\mathrm{mod}\,23) \equiv 11(\mathrm{mod}\,23)$,

$11^2(\mathrm{mod}\,23) \equiv 6(\mathrm{mod}\,23)$,

$6^2(\mathrm{mod}\,23) \equiv 13(\mathrm{mod}\,23)$,

$13 \cdot 19(\mathrm{mod}\,23) \equiv 17(\mathrm{mod}\,23)$.

Итак, $19^{-1}(\mathrm{mod}\,23) = 17$. Тогда $q \equiv 9 \cdot 17(\mathrm{mod}\,23) \equiv 15(\mathrm{mod}\,23)$ или $q = 15 + 23s$, $s \in Z$.

Решением первых двух сравнений является $K' = 3 + 19(15 + 23s) = 288 + 437s$, $s \in Z$, или $K' \equiv 288(\mathrm{mod}\,437)$.

Находим значение K', удовлетворяющее сравнению $K' \equiv 288(\mathrm{mod}\,437)$ и третьему сравнению системы (30). Имеем $K' = 288 + 437s \equiv 15(\mathrm{mod}\,31)$ или $437s \equiv -273(\mathrm{mod}\,31)$. Так как $437 \equiv 3(\mathrm{mod}\,31)$, а $-273 \equiv 6(\mathrm{mod}\,31)$, то $3s \equiv 6(\mathrm{mod}\,31)$ или $s \equiv 2(\mathrm{mod}\,31)$. Следовательно, $s = 2 + 31t$, $t \in Z$, и решением трех сравнений является $K' = 288 + 437(2 + 31t) = 1162 + 13547t$, $t \in Z$ то есть решением системы (30) является $K' \equiv 1162(\mathrm{mod}\,13547)$. Отсюда ключ $K = K' - r \cdot p = 1162 - 105 \cdot 11 = 7$.

Список использованных источников

1. Акритас, А. Основы компьютерной алгебры с приложениями / А. Акритас. – М.: Мир, 1994. – 544 с.

2. Бухштаб, А.А. Теория чисел: учеб. пособие для вузов / А. А. Бухштаб. – СПб.: Лань, 2015. – 383 с.

3. Виноградов, И. М. Основы теории чисел: учеб. пособие / И. М. Виноградов. – СПб.: Лань, 2009. – 176 с.

4. Герман, О.Н. Теоретико-числовые методы в криптографии: учебник для студ. учреждений высш. проф. Образования / О.Н. Герман, Ю.В. Нестеренко. – М.: Издательский центр «Академия», 2012 – 272 с.

5. Отрыванкина, Т. М. Алгоритмы компьютерной алгебры: практикум / Т. М. Отрыванкина. – Оренбург: ОГУ, 2007. – 26 с.

6. Судоплатов, С. В. Дискретная математика: учебник / С. В. Судоплатов, Е. В. Овчинникова. – Новосибирск: Изд-во НГТУ, 2012. – 280 с.

Приложение А

(справочное)

Таблица простых чисел

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53
59	61	67	71	73	79	83	89	97	101	103	107	109	113	127	131
137	139	149	151	157	163	167	173	179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263	269	271	277	281	283	293	307	311
313	317	331	337	347	349	353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569	571	577	587	593	599	601	607	613
617	619	631	641	643	647	653	659	661	673	677	683	691	701	709	719
727	733	739	743	751	757	761	769	773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997	1009	1013	1019	1021	1031	1033	1039	1049
1051	1061	1063	1069	1087	1091	1093	1097	1103	1109	1117	1123	1129	1151	1153	1163
1171	1181	1187	1193	1201	1213	1217	1223	1229	1231	1237	1249	1259	1277	1279	1283
1289	1291	1297	1301	1303	1307	1319	1321	1327	1361	1367	1373	1381	1399	1409	1423
1427	1429	1433	1439	1447	1451	1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583	1597	1601	1607	1609	1613	1619
1621	1627	1637	1657	1663	1667	1669	1693	1697	1699	1709	1721	1723	1733	1741	1747
1753	1759	1777	1783	1787	1789	1801	1811	1823	1831	1847	1861	1867	1871	1873	1877
1879	1889	1901	1907	1913	1931	1933	1949	1951	1973	1979	1987	1993	1997	1999	2003
2011	2017	2027	2029	2039	2053	2063	2069	2081	2083	2087	2089	2099	2111	2113	2129
2131	2137	2141	2143	2153	2161	2179	2203	2207	2213	2221	2237	2239	2243	2251	2267
2269	2273	2281	2287	2293	2297	2309	2311	2333	2339	2341	2347	2351	2357	2371	2377
2381	2383	2389	2393	2399	2411	2417	2423	2437	2441	2447	2459	2467	2473	2477	2503
2521	2531	2539	2543	2549	2551	2557	2579	2591	2593	2609	2617	2621	2633	2647	2657
2659	2663	2671	2677	2683	2687	2689	2693	2699	2707	2711	2713	2719	2729	2731	2741
2749	2753	2767	2777	2789	2791	2797	2801	2803	2819	2833	2837	2843	2851	2857	2861
2879	2887	2897	2903	2909	2917	2927	2939	2953	2957	2963	2969	2971	2999	3001	3011
3019	3023	3037	3041	3049	3061	3067	3079	3083	3089	3109	3119	3121	3137	3163	3167
3169	3181	3187	3191	3203	3209	3217	3221	3229	3251	3253	3257	3259	3271	3299	3301
3307	3313	3319	3323	3329	3331	3343	3347	3359	3361	3371	3373	3389	3391	3407	3413
3433	3449	3457	3461	3463	3467	3469	3491	3499	3511	3517	3527	3529	3533	3539	3541
3547	3557	3559	3571	3581	3583	3593	3607	3613	3617	3623	3631	3637	3643	3659	3671
3673	3677	3691	3697	3701	3709	3719	3727	3733	3739	3761	3767	3769	3779	3793	3797
3803	3821	3823	3833	3847	3851	3853	3863	3877	3881	3889	3907	3911	3917	3919	3923
3929	3931	3943	3947	3967	3989	4001	4003	4007	4013	4019	4021	4027	4049	4051	4057

4073	4079	4091	4093	4099	4111	4127	4129	4133	4139	4153	4157	4159	4177	4201	4211
4217	4219	4229	4231	4241	4243	4253	4259	4261	4271	4273	4283	4289	4297	4327	4337
4339	4349	4357	4363	4373	4391	4397	4409	4421	4423	4441	4447	4451	4457	4463	4481
4483	4493	4507	4513	4517	4519	4523	4547	4549	4561	4567	4583	4591	4597	4603	4621
4637	4639	4643	4649	4651	4657	4663	4673	4679	4691	4703	4721	4723	4729	4733	4751
4759	4783	4787	4789	4793	4799	4801	4813	4817	4831	4861	4871	4877	4889	4903	4909
4919	4931	4933	4937	4943	4951	4957	4967	4969	4973	4987	4993	4999	5003	5009	5011
5021	5023	5039	5051	5059	5077	5081	5087	5099	5101	5107	5113	5119	5147	5153	5167
5171	5179	5189	5197	5209	5227	5231	5233	5237	5261	5273	5279	5281	5297	5303	5309
5323	5333	5347	5351	5381	5387	5393	5399	5407	5413	5417	5419	5431	5437	5441	5443
5449	5471	5477	5479	5483	5501	5503	5507	5519	5521	5527	5531	5557	5563	5569	5573
5581	5591	5623	5639	5641	5647	5651	5653	5657	5659	5669	5683	5689	5693	5701	5711
5717	5737	5741	5743	5749	5779	5783	5791	5801	5807	5813	5821	5827	5839	5843	5849
5851	5857	5861	5867	5869	5879	5881	5897	5903	5923	5927	5939	5953	5981	5987	6007
6011	6029	6037	6043	6047	6053	6067	6073	6079	6089	6091	6101	6113	6121	6131	6133
6143	6151	6163	6173	6197	6199	6203	6211	6217	6221	6229	6247	6257	6263	6269	6271
6277	6287	6299	6301	6311	6317	6323	6329	6337	6343	6353	6359	6361	6367	6373	6379
6389	6397	6421	6427	6449	6451	6469	6473	6481	6491	6521	6529	6547	6551	6553	6563
6569	6571	6577	6581	6599	6607	6619	6637	6653	6659	6661	6673	6679	6689	6691	6701
6703	6709	6719	6733	6737	6761	6763	6779	6781	6791	6793	6803	6823	6827	6829	6833
6841	6857	6863	6869	6871	6883	6899	6907	6911	6917	6947	6949	6959	6961	6967	6971
6977	6983	6991	6997	7001	7013	7019	7027	7039	7043	7057	7069	7079	7103	7109	7121
7127	7129	7151	7159	7177	7187	7193	7207	7211	7213	7219	7229	7237	7243	7247	7253
7283	7297	7307	7309	7321	7331	7333	7349	7351	7369	7393	7411	7417	7433	7451	7457
7459	7477	7481	7487	7489	7499	7507	7517	7523	7529	7537	7541	7547	7549	7559	7561
7573	7577	7583	7589	7591	7603	7607	7621	7639	7643	7649	7669	7673	7681	7687	7691
7699	7703	7717	7723	7727	7741	7753	7757	7759	7789	7793	7817	7823	7829	7841	7853
7867	7873	7877	7879	7883	7901	7907	7919	7927	7933	7937	7949	7951	7963	7993	8009
8011	8017	8039	8053	8059	8069	8081	8087	8089	8093	8101	8111	8117	8123	8147	8161
8167	8171	8179	8191	8209	8219	8221	8231	8233	8237	8243	8263	8269	8273	8287	8291
8293	8297	8311	8317	8329	8353	8363	8369	8377	8387	8389	8419	8423	8429	8431	8443
8447	8461	8467	8501	8513	8521	8527	8537	8539	8543	8563	8573	8581	8597	8599	8609
8623	8627	8629	8641	8647	8663	8669	8677	8681	8689	8693	8699	8707	8713	8719	8731
8737	8741	8747	8753	8761	8779	8783	8803	8807	8819	8821	8831	8837	8839	8849	8861
8863	8867	8887	8893	8923	8929	8933	8941	8951	8963	8969	8971	8999	9001	9007	9011
9013	9029	9041	9043	9049	9059	9067	9091	9103	9109	9127	9133	9137	9151	9157	9161
9173	9181	9187	9199	9203	9209	9221	9227	9239	9241	9257	9277	9281	9283	9293	9311
9319	9323	9337	9341	9343	9349	9371	9377	9391	9397	9403	9413	9419	9421	9431	9433
9437	9439	9461	9463	9467	9473	9479	9491	9497	9511	9521	9533	9539	9547	9551	9587
9601	9613	9619	9623	9629	9631	9643	9649	9661	9677	9679	9689	9697	9719	9721	9733
9739	9743	9749	9767	9769	9781	9787	9791	9803	9811	9817	9829	9833	9839	9851	9857
9859	9871	9883	9887	9901	9907	9923	9929	9931	9941	9949	9967	9973			

Приложение Б

(справочное)

Символ Лежандра и его свойства

Определение символа Лежандра. Для любого простого нечетного p и целого a символ Лежандра определяется следующим образом:

$$\left(\frac{a}{p}\right)=\begin{cases}0, \ \textit{если} \ a\equiv 0(\bmod p),\\ 1, \ \textit{если} \ a-\textit{вычет} \ (\bmod p),\\ -1, \textit{если} \ a-\textit{невычет} \ (\bmod p).\end{cases}$$

Свойства символа Лежандра:

1. $a_1 \equiv a(mod\ p) \Rightarrow \left(\frac{a}{p}\right)=\left(\frac{a_1}{p}\right)$.

2. Критерий Эйлера. $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}\ (mod\ p)$.

3. $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$.

4. $Если\ \ НОД(a,p)=1 \Rightarrow \left(\frac{a^2b}{p}\right)=\left(\frac{b}{p}\right)$.

5. $\left(\frac{1}{p}\right)=1, \left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

6. $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1, & p\equiv\pm 1(\bmod 8),\\ -1, & p\equiv\pm 3(\bmod 8).\end{cases}$

7. Квадратичный закон взаимности. Для любых простых нечетных p и q справедливо $\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)$.