Discrete Mathematics

Number Theory and Cryptography

Myles Moylan

4.1 Divisibility and Modular Arithmetic

1. Does 17 divide each of these numbers?

a) 68
Yes, since $68 = 17 \cdot 4$.

b) 84
No, it has a remainder of 16.

c) 357
Yes, since $357 = 17 \cdot 21$.

d) 1001
No, it has a remainder of 15.

2. Show that if $a|b$ and $b|a$, where a and b are integers, then $a = b$ or $a = -b$.

The given conditions imply that there are integers s and t such that $a = bs$ and $b = at$. Combining these, we obtain $a = ats$; and since $a \neq 0$, we conclude that $st = 1$. Now the only way for this to happen is for $s = t = 1$ or $s = t = -1$. Therefore either $a = b$ or $a = -b$.

3. Show that if a, b, and c are integers, where $a \neq 0$ and $c \neq 0$, such that $ac|bc$, then $a|b$.

The given condition means that $bc = (ac)t$ for some integer t. Since $c \neq 0$, we can divide both sides by c to obtain $b = at$. This is the definition of $a|b$, as desired.

4. Prove that if a and b are integers and a divides b, then a is odd or b is even.

It is given that a and b are integers and a divides b, so $b = ma$ for some integer m. We consider two cases: either a is odd or a is not odd. If a is odd, then the conclusion of the implication holds. If a is not odd, then it is even and $a = 2k$ for some integer k, whence $b = 2km$. This means by definition b is even.

5. What are the quotient and remainder when

a) 19 is divided by 7?
$19 = 7 \cdot 2 + 5$, so $q = 2$ and $r = 5$

b) -111 is divided by 11?
$-111 = 11 \cdot (-11) + 10$, so $q = -11$ and $r = 10$

c) 789 is divided by 23?
$789 = 23 \cdot 34 + 7$, so $q = 34$ and $r = 7$

d) 1001 is divided by 13?
$1001 = 13 \cdot 77 + 0$, so $q = 77$ and $r = 0$

e) 0 is divided by 19?
$0 = 19 \cdot 0 + 0$, so $q = 0$ and $r = 0$

f) 3 is divided by 5?
$3 = 5 \cdot 0 + 3$, so $q = 0$ and $r = 3$

g) -1 is divided by 3?
$-1 = 3 \cdot (-1) + 2$, so $q = -1$ and $r = 2$

h) 4 is divided by 1?
$4 = 1 \cdot 4 + 0$, so $q = 4$ and $r = 0$

6. What time does a 12-hour clock read

a) 80 hours after it reads 11:00?
$11 + 80 \bmod 12 = 7$, so the clock reads 7:00.

b) 40 hours before it reads 12:00?
$12 - 40 \bmod 12 = 8$, so the clock reads 8:00.

c) 100 hours after it reads 6:00?
$6 + 100 \bmod 12 = 10$, so the clock reads 10:00.

7. What time does a 24-hour clock read

a) 100 hours after it reads 2:00?
$2 + 100 \bmod 24 = 6$, so the clock reads 6:00.

b) 45 hours before it reads 12:00?
$12 - 45 \bmod 24 = 15$, so the clock reads 15:00.

c) 168 hours after it reads 19:00?
$19 - 168 \bmod 24 = 19$, so the clock reads 19:00.

8. Suppose that a and b are integers, $a \equiv 4 \pmod{13}$, and $b \equiv 9 \pmod{13}$. Find the integer c with $0 \leq c \leq 12$ such that

a) $c \equiv 9a \pmod{13}$.
$9 \cdot 4 \bmod 13 = 36 \bmod 13 = 10$

b) $c \equiv 11b \pmod{13}$.
$11 \cdot 9 \bmod 13 = 99 \bmod 13 = 8$

c) $c \equiv a + b \pmod{13}$.
$4 + 9 \bmod 13 = 13 \bmod 13 = 0$

d) $c \equiv 2a + 3b \pmod{13}$.
$2 \cdot 4 + 3 \cdot 9 \bmod 13 = 35 \bmod 13 = 9$

e) $c \equiv a^2 + b^2 \pmod{13}$.
$4^2 + 9^2 \bmod 13 = 97 \bmod 13 = 6$

f) $c \equiv a^3 - b^3 \pmod{13}$.
$4^3 - 9^3 \bmod 13 = -665 \bmod 13 = 11$

9. Suppose that a and b are integers, $a \equiv 11 \pmod{19}$, and $b \equiv 3 \pmod{19}$. Find the integer c with $0 \leq c \leq 18$ such that

a) $c \equiv 13a \pmod{19}$.
$13 \cdot 11 \bmod 19 = 143 \bmod 19 = 10$

b) $c \equiv 8b \pmod{19}$.
$8 \cdot 3 \bmod 19 = 24 \bmod 19 = 5$

c) $c \equiv a - b \pmod{19}$.
$11 - 3 \bmod 19 = 8 \bmod 19 = 8$

d) $c \equiv 7a + 3b \pmod{19}$.
$7 \cdot 11 + 3 \cdot 3 \bmod 19 = 86 \bmod 19 = 10$

e) $c \equiv 2a^2 + 3b^2 \pmod{19}$.
$2 \cdot 11^2 + 3 \cdot 3^2 \bmod 19 = 296 \bmod 19 = 11$

f) $c \equiv a^3 + 4b^3 \pmod{19}$.
$11^3 + 4 \cdot 3^3 \bmod 19 = 1439 \bmod 19 = 14$

10. Let m be a positive integer. Show that $a \equiv b \pmod{m}$ if $a \bmod m = b \bmod m$.

The given condition, that $a \bmod m = b \bmod m$, means that a and b have the same remainder when divided by m. In symbols, $a = q_1 m + r$ and $b = q_2 m + r$ for some integers q_1, q_2, and r. Subtracting these two equations gives us $a - b = (q_1 - q_2)m$, which says that m divides (is a factor of) $a - b$. This is precisely the definition of $a \equiv b \pmod{m}$.

11. Evaluate these quantities.

a) $-17 \bmod 2$
$-17 = 2 \cdot (-8) + (-1)$, so $-17 \bmod 2 = 1$

b) $144 \bmod 7$
$144 = 7 \cdot 20 + 4$, so $144 \bmod 7 = 4$

c) $-101 \bmod 19$
$-101 = 19 \cdot (-5) + (-6)$, so $-101 \bmod 19 = 19 + (-6) = 13$

d) $199 \bmod 19$
$199 = 19 \cdot 10 + 9$, so $199 \bmod 19 = 9$

e) $13 \bmod 3$
$13 = 3 \cdot 4 + 1$, so $13 \bmod 3 = 1$

f) $-97 \bmod 11$
$-97 = 11 \cdot (-9) + 2$, so $-97 \bmod 11 = 2$

g) $155 \bmod 19$
$155 = 19 \cdot 8 + 3$, so $155 \bmod 19 = 3$

h) $-221 \bmod 23$
$-221 = 23 \cdot (-10) + 9$, so $-221 \bmod 23 = 9$

12. Find integer a such that

a) $a \equiv 43 \pmod{23}$ and $-22 \leq a \leq 0$.
$a = 43 - 23 \cdot 2 = -3$

b) $a \equiv 17 \pmod{29}$ and $-14 \leq a \leq 14$.
$a = 17 - 29 = -12$

c) $a \equiv -11 \pmod{21}$ and $90 \leq a \leq 110$.
$a = -11 + 21 \cdot 5 = 94$

d) $a \equiv -15 \pmod{27}$ and $-26 \leq a \leq 0$.
$a = -15$

e) $a \equiv 24 \pmod{31}$ and $-15 \leq a \leq 15$.
$a = 24 - 31 = -7$

f) $a \equiv 99 \pmod{41}$ and $100 \leq a \leq 140$.
$a = 99 + 41 = 140$

4.2 Integer Representations and Algorithms

1. Convert the decimal expansion of each of these integers to a binary expansion.

a) 231

$231/2 = 115$, $231 \bmod 2 = 1$
$115/2 = 57$, $115 \bmod 2 = 1$
$57/2 = 28$, $57 \bmod 2 = 1$
$28/2 = 14$, $28 \bmod 2 = 0$
$14/2 = 7$, $14 \bmod 2 = 0$
$7/2 = 3$, $7 \bmod 2 = 1$
$3/2 = 1$, $3 \bmod 2 = 1$
$1/2 = 0$, $1 \bmod 2 = 1$

$231 = (11100111)_2$.

b) 4532

$4532/2 = 2266$, $4532 \bmod 2 = 0$
$2266/2 = 1133$, $2266 \bmod 2 = 0$
$1133/2 = 566$, $1133 \bmod 2 = 1$
$566/2 = 283$, $566 \bmod 2 = 0$
$283/2 = 141$, $283 \bmod 2 = 1$
$141/2 = 70$, $141 \bmod 2 = 1$
$70/2 = 35$, $70 \bmod 2 = 0$
$35/2 = 17$, $35 \bmod 2 = 1$
$17/2 = 8$, $17 \bmod 2 = 1$
$8/2 = 4$, $8 \bmod 2 = 0$
$4/2 = 2$, $4 \bmod 2 = 0$
$2/2 = 1$, $2 \bmod 2 = 0$
$1/2 = 0$, $1 \bmod 2 = 1$

$4532 = (1000110110100)_2$

c) 97644

$97644/2 = 48822$, $97644 \bmod 2 = 0$
$48822/2 = 24411$, $48822 \bmod 2 = 0$
$24411/2 = 12205$, $24411 \bmod 2 = 1$
$12205/2 = 6102$, $12205 \bmod 2 = 1$
$6102/2 = 3051$, $6102 \bmod 2 = 0$
$3051/2 = 1525$, $3051 \bmod 2 = 1$
$1525/2 = 762$, $1525 \bmod 2 = 1$
$762/2 = 381$, $762 \bmod 2 = 0$
$381/2 = 190$, $381 \bmod 2 = 1$
$190/2 = 95$, $190 \bmod 2 = 0$
$95/2 = 47$, $95 \bmod 2 = 1$
$47/2 = 23$, $47 \bmod 2 = 1$
$23/2 = 11$, $23 \bmod 2 = 1$
$11/2 = 5$, $11 \bmod 2 = 1$
$5/2 = 2$, $5 \bmod 2 = 1$
$2/2 = 1$, $2 \bmod 2 = 0$
$1/2 = 0$, $1 \bmod 2 = 1$

$97644 = (10111110101101100)_2$

d) 321

$321/2 = 160$, $321 \bmod 2 = 1$

$160/2 = 80$, $160 \bmod 2 = 0$

$80/2 = 40$, $80 \bmod 2 = 0$

$40/2 = 20$, $40 \bmod 2 = 0$

$20/2 = 10$, $20 \bmod 2 = 0$

$10/2 = 5$, $10 \bmod 2 = 0$

$5/2 = 2$, $5 \bmod 2 = 1$

$2/2 = 1$, $2 \bmod 2 = 0$

$1/2 = 0$, $1 \bmod 2 = 1$

$321 = (101000001)_2$

e) 1023

$1023/2 = 511$, $1023 \bmod 2 = 1$

$511/2 = 255$, $511 \bmod 2 = 1$

$255/2 = 127$, $255 \bmod 2 = 1$

$127/2 = 63$, $127 \bmod 2 = 1$

$63/2 = 31$, $63 \bmod 2 = 1$

$31/2 = 15$, $31 \bmod 2 = 1$

$15/2 = 7$, $15 \bmod 2 = 1$

$7/2 = 3$, $7 \bmod 2 = 1$

$3/2 = 1$, $3 \bmod 2 = 1$

$1/2 = 0$, $1 \bmod 2 = 1$

$1023 = (1111111111)_2$

f) 100632

$100632/2 = 50316$, $100632 \bmod 2 = 0$

$50316/2 = 25158$, $50316 \bmod 2 = 0$

$25158/2 = 12579$, $25158 \bmod 2 = 0$

$12579/2 = 6289$, $12579 \bmod 2 = 1$

$6289/2 = 3144$, $6289 \bmod 2 = 1$

$3144/2 = 1572$, $3144 \bmod 2 = 0$

$1572/2 = 786$, $1572 \bmod 2 = 0$

$786/2 = 393$, $786 \bmod 2 = 0$

$393/2 = 196$, $393 \bmod 2 = 1$

$196/2 = 98$, $196 \bmod 2 = 0$

$98/2 = 49$, $98 \bmod 2 = 0$

$49/2 = 24$, $49 \bmod 2 = 1$

$24/2 = 12$, $24 \bmod 2 = 0$

$12/2 = 6$, $12 \bmod 2 = 0$

$6/2 = 3$, $6 \bmod 2 = 0$

$3/2 = 1$, $3 \bmod 2 = 1$

$1/2 = 0$, $1 \bmod 2 = 1$

$100632 = (11000100100011000)_2$

2. Convert the binary expansion of each of these integers to a decimal expansion.

a) $(11111)_2 = 31$

b) $(1000000001)_2 = 513$

c) $(101010101)_2 = 341$

d) $(110100100010000)_2 = 26896$

e) $(11011)_2 = 27$

f) $(1010110101)_2 = 693$

g) $(1110111110)_2 = 958$

h) $(111110000011111)_2 = 31775$

3. Convert the octal expansion of each of these integers to a binary expansion.

a) $(572)_8 = (101111010)_2$

b) $(1604)_8 = (1110000100)_2$

c) $(423)_8 = (100010011)_2$

d) $(2417)_8 = (10100001111)_2$

4. Convert the binary expansion of each of these integers to an octal expansion.

a) $(11110111)_2 = (367)_8$

b) $(101010101010)_2 = (5252)_8$

c) $(111011101110111)_2 = (73567)_8$

d) $(101010101010101)_2 = (52525)_8$

5. Convert the hexadecimal expansion of each of these integers to a binary expansion.

a) $(80E)_{16} = (100000001110)_2$

b) $(135AB)_{16} = (10011010110101011)_2$

c) $(ABBA)_{16} = (1010101110111010)_2$

d) $(DEFACED)_{16} = (1101111011111010110011101101)_2$

6. Convert $(BADFACED)_{16}$ from its hexadecimal expansion to its binary expansion.

$(BADFACED)_{16} = (10111010110111111010110011101101)_2$

7. Convert $(ABCDEF)_{16}$ from its hexadecimal expansion to its binary expansion.

$(ABCDEF)_{16} = (101010111100110111101111)_2$

8. Convert $(101101111011)_2$ from its binary expansion to its hexadecimal expansion.

$(101101111011)_2 =(B7B)_{16}$

9. Convert $(1100001100011)_2$ from its binary expansion to its hexadecimal expansion.

$(1100001100011)_2 = (1863)_{16}$

10. Find the sum and the product of each of these pairs of numbers. Express your answers as a binary expansion.

a) $(1000111)_2$, $(1110111)_2$

$1000111 + 1110111 = 10111110$

$1000111 \cdot 1110111 = 10000100000001$

b) $(11101111)_2$, $(10111101)_2$

$11101111 + 10111101 = 110101100$

$11101111 \cdot 10111101 = 1011000001110011$

c) $(1010101010)_2$, $(111110000)_2$

$1010101010 + 111110000 = 10010011010$

$1010101010 \cdot 111110000 = 1010010100101100000$

d) $(1000000001)_2$, $(1111111111)_2$

$1000000001 + 1111111111 = 11000000000$

$1000000001 \cdot 1111111111 = 10000000000111111111$

11. Use the fast modular exponentiation algorithm to find

a) $7^{644} \bmod 645 = 436$

b) $11^{644} \bmod 645 = 1$

c) $3^{2003} \bmod 99 = 27$

d) $123^{1001} \bmod 101 = 22$

4.3 Primes and Greatest Common Divisors

1. Determine whether each of these integers is prime.

a) 21

Since $21 = 3 \cdot 7$, we know that 21 is not prime.

b) 29

Since $2 \not| 29$, $3 \not| 29$, and $5 \not| 29$, we know that 29 is prime. We needed to check for prime divisors only up to $\sqrt{29}$, which is less than 6.

c) 71

Since $2 \not| 71$, $3 \not| 71$, $5 \not| 71$, and $7 \not| 71$, we know that 71 is prime.

d) 97

Since $2 \not| 97$, $3 \not| 97$, $5 \not| 97$, and $7 \not| 97$, we know that 97 is prime.

e) 111

Since $111 = 3 \cdot 37$, we know that 111 is not prime.

f) 143

Since $143 = 11 \cdot 13$, we know that 143 is not prime.

2. Find the prime factorization of each of these integers.

a) 88

$88 = 2 \cdot 2 \cdot 2 \cdot 11 = 2^3 \cdot 11$

b) 126

$126 = 2 \cdot 63 = 2 \cdot 3 \cdot 21 = 2 \cdot 3 \cdot 3 \cdot 7 = 2 \cdot 3^2 \cdot 7$

c) 729

$729 = 3 \cdot 243 = 3 \cdot 3 \cdot 81 = 3 \cdot 3 \cdot 3 \cdot 27 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 9 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = 3^6$

d) 1001

$1001 = 7 \cdot 143 = 7 \cdot 11 \cdot 13$

e) 1111

$1111 = 11 \cdot 101$

f) 909,090

$909090 = 2 \cdot 454545 = 2 \cdot 3 \cdot 151515 = 2 \cdot 3 \cdot 3 \cdot 50505 = 2 \cdot 3 \cdot 3 \cdot 3 \cdot 16835 = 2 \cdot 3 \cdot 3 \cdot \cdot 5 \cdot 3367 = 2 \cdot 3 \cdot 3 \cdot \cdot 5 \cdot 7 \cdot 481 = 2 \cdot 3 \cdot 3 \cdot \cdot 5 \cdot 7 \cdot 13 \cdot 37 = 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 37$

3. Express in pseudocode the trial division algorithm for determining whether an integer is prime.

```
procedure primetester(n : integer greater than 1)
isprime := true
d := 2
while isprime and $d \leq \sqrt{n}$
    if $n \bmod d = 0$ then isprime := false
    else $d := d + 1$
return isprime
```

4. Which positive integers less than 30 are relatively prime to 30?

The prime factors of 30 are 2, 3, and 5. Thus we are looking for positive integers less than 30 that have none of these as prime factors. Since the smallest prime number other than these is 7, and 7^2 is already greater than 30, in fact only primes (and the number 1) will satisfy this condition. Therefore the answer is 1, 7, 11, 13, 17, 19, 23, and 29.

5. Which positive integers less than 12 are relatively prime to 12?

The prime factors of 12 are 2 and 3. So the answer is 1, 5, 7, and 11.

6. Determine whether the integers in each of these sets are pairwise relatively prime.

a) 11, 15, 19
Since $\gcd(11, 15) = 1$, $\gcd(11, 19) = 1$, and $\gcd(15, 19) = 1$, these three numbers are pairwise relatively prime.

b) 14, 15, 21
Since $\gcd(15, 21) = 3 > 1$, these three numbers are not pairwise relatively prime.

c) 12, 17, 31, 37
Since $\gcd(12, 17) = 1$, $\gcd(12, 31) = 1$, $\gcd(12, 37) = 1$, $\gcd(17, 31) = 1$, $\gcd(17, 37) = 1$, and $\gcd(31, 37) = 1$, these four numbers are pairwise relatively prime.

d) 7, 8, 9, 11
Since no two of 7, 8, 9, and 11 have a common factor greater than 1, this set is pairwise relatively prime.

7. Find these values of the Euler ϕ-function.

a) $\phi(4) = |\{1, 3\}| = 2$

b) $\phi(10) = |\{1, 3, 7, 9\}| = 4$

c) $\phi(13) = |\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}| = 12$

8. Show that n is prime if and only if $\phi(n) = n - 1$.

Since a prime number is divisible only by itself and 1, and the Euler ϕ-function at the positive integer n is defined to be the number of positive integers less than or equal to n that are relatively prime to n, it follows that all the numbers less than n will be relatively prime to n, resulting in $\phi(n) = n - 1$.

9. What is the value of $\phi(p^k)$ when p is prime and k is a positive integer?

All the positive integers less than or equal to p^k (and there are clearly p^k of them) are less than p^k and relatively prime to p^k unless they are a multiple of p. Since the fraction $1/p$ of them are multiples of p, we have $\phi(p^k) = p^k(1 - 1/p) = p^k - p^{k-1}$.

10. What are the greatest common divisors of these pairs of integers?

a) $3^7 \cdot 5^3 \cdot 7^3$, $2^{11} \cdot 3^5 \cdot 5^9$
$\gcd = 2^{\min(0,11)} \cdot 3^{\min(7,5)} \cdot 5^{\min(3,9)} \cdot 7^{\min(3,0)} = 3^5 \cdot 5^3$

b) $11 \cdot 13 \cdot 17$, $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$
Since these numbers have no common prime factors, $\gcd = 1$.

c) 23^{31}, 23^{17}
$\gcd = 23^{\min(31,17)} = 23^{17}$

d) $41 \cdot 43 \cdot 53$, $41 \cdot 43 \cdot 53$
$\gcd = 41 \cdot 43 \cdot 53$

e) $3^{13} \cdot 5^{17}$, $2^{12} \cdot 7^{21}$
Since these numbers have no common prime factors, $\gcd = 1$.

f) 1111, 0
The gcd of any positive integer and 0 is that integer, so $\gcd = 1111$.

11. What are the least common multiples of each of these pairs of integers?

a) $3^7 \cdot 5^3 \cdot 7^3$, $2^{11} \cdot 3^5 \cdot 5^9$
$\text{lcm} = 2^{\max(0,11)} \cdot 3^{\max(7,5)} \cdot 5^{\max(3,9)} \cdot 7^{\max(3,0)} = 2^{11} \cdot 3^7 \cdot 5^9 \cdot 7^3$

b) $11 \cdot 13 \cdot 17$, $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$
Since these numbers have no common prime factors the lcm is their product: $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17$.

c) 23^{31}, 23^{17}
$\text{lcm} = 23^{\max(31,17)} = 23^{31}$

d) $41 \cdot 43 \cdot 53$, $41 \cdot 43 \cdot 53$
$\text{lcm} = 41 \cdot 43 \cdot 53$

e) $3^{13} \cdot 5^{17}$, $2^{12} \cdot 7^{21}$
Since these numbers have no common prime factors the lcm is their product: $2^{12} \cdot 3^{13} \cdot 5^{17} \cdot 7^{21}$

f) 1111, 0
It makes no sense to ask for a positive multiple of 0, so this question has no answer. Lease common multiples are defined only for positive integers.

12. If the product of two integers is $2^7 \cdot 3^8 \cdot 5^2 \cdot 7^{11}$ and their greatest common divisor is $2^3 \cdot 3^4 \cdot 5$, what is their least common multiple?

First, we compare the product and gcd to find each integer as it stands:

$2^{7-3} = 2^4 \implies 2^4,\ 2^3$
$3^{8-4} = 3^4 \implies 3^4,\ 3^4$
$5^{2-1} = 5^1 \implies 5,\ 5$
$7^{11-0} = 7^{11} \implies 7^{11},\ 1$

It follows that: $\text{lcm} = 2^{\max(4,3)} \cdot 3^{\max(4,4)} \cdot 5^{\max(1,1)} \cdot 7^{\max(11,0)} = 2^4 \cdot 3^4 \cdot 5 \cdot 7^{11}$

13. Show that if a and b are positive integers, then $ab = \gcd(a,b) \cdot \text{lcm}(a,b)$.

Since the exponent of the prime p in $\gcd(a,b)$ is the smaller of the exponents of p in a and in b, and since the exponent of the prime p in $\text{lcm}(a,b)$ is the larger of the exponents of p in a and in b, the exponent of p in $\gcd(a,b) \cdot \text{lcm}(a,b)$ is the sum of the smaller and the larger of these two values. Therefore by the observation, it equals the sum of the two values themselves, which is clearly equal to the exponent of p in ab. Since this is true for every prime p, we conclude that $\gcd(a,b) \cdot \text{lcm})(a,b)$ and ab have the same prime factorization and are therefore equal.

14. Use the Euclidean algorithm to find

a) $\gcd(12,18) = \gcd(12,6) = \gcd(6,0) = 6$

b) $\gcd(111,201) = \gcd(111,90) = \gcd(90,21) = \gcd(21,6) = \gcd(6,3) = \gcd(3,0) = 3$

c) $\gcd(1001,1331) = \gcd(1001,330) = \gcd(330,11) = \gcd(11,0) = 11$

d) $\gcd(12345,54321) = \gcd(12345,4941) = \gcd(4941,2463) = \gcd(2463,15) = \gcd(15,3) = \gcd(3,0) = 3$

e) $\gcd(1000,5040) = \gcd(1000,40) = \gcd(40,0) = 40$

f) $\gcd(9888,6060) = \gcd(6060,3828) = \gcd(3828,2232) = \gcd(2232,1596) = \gcd(1596,636) = \gcd(636,324) = \gcd(324,312) = \gcd(312,12) = \gcd(12,0) = 12$

15. How many divisions are required to find $\gcd(34,55)$ using the Euclidean algorithm?

In carrying out the Euclidean algorithm, we divide successively by 55, 34, 21, 13, 8, 5, 3, 2, and 1, resulting in nine divisions.

4.4 Solving Congruences

1. Show that 15 is an inverse of 7 modulo 26.

We need to show that $15 \cdot 7 \equiv 1 \pmod{26}$ or that $15 \cdot 7 - 1$ is divisible by 26. Indeed, $15 \cdot 7 - 1 = 104$ and $104 = 26 \cdot 4$.

2. Show that 937 is an inverse of 13 modulo 2436.

We need to show that $937 \cdot 13 \equiv 1 \pmod{2436}$ or that $937 \cdot 13 - 1$ is divisible by 2436. Indeed, $937 \cdot 13 - 1 = 12180$ and $12180 = 2436 \cdot 5$.

3. By inspection, find an inverse of 4 modulo 9.

We want to find an integer k such that $4k$ is 1 greater than a multiple of 9.

$$\begin{aligned}
&4 \cdot 1 = 4 = 0 \cdot 9 + 4\\
&4 \cdot 2 = 8 = 0 \cdot 9 + 8\\
&4 \cdot 3 = 12 = 1 \cdot 9 + 3\\
&4 \cdot 4 = 16 = 1 \cdot 9 + 7\\
&4 \cdot 5 = 20 = 2 \cdot 9 + 2\\
&4 \cdot 6 = 24 = 2 \cdot 9 + 6\\
&4 \cdot 7 = 28 = 3 \cdot 9 + 1
\end{aligned}$$

Therefore an inverse of 4 modulo 9 is 7.

4. By inspection, find an inverse of 2 modulo 17.

We want to find an integer k such that $2k$ is 1 greater than a multiple of 17.

$$\begin{aligned}
&2 \cdot 1 = 2 = 0 \cdot 17 + 2\\
&2 \cdot 2 = 4 = 0 \cdot 17 + 4\\
&2 \cdot 3 = 6 = 0 \cdot 17 + 6\\
&2 \cdot 4 = 8 = 0 \cdot 17 + 8\\
&2 \cdot 5 = 10 = 0 \cdot 17 + 10\\
&2 \cdot 6 = 12 = 0 \cdot 17 + 12\\
&2 \cdot 7 = 14 = 0 \cdot 17 + 14\\
&2 \cdot 8 = 16 = 0 \cdot 17 + 16\\
&2 \cdot 9 = 18 = 1 \cdot 17 + 1
\end{aligned}$$

Therefore an inverse of 2 modulo 17 is 9.

5. Find an inverse of a modulo m for each of these pairs of relatively prime integers.

a) $a = 4$, $m = 9$

First, we carry out the Euclidean algorithm to find $\gcd(4, 9)$:

$$9 = 2 \cdot 4 + 1$$
$$4 = 4 \cdot 1$$

Then we work backwards to rewrite the gcd (the last nonzero remainder, which is 1 here) in terms of 4 and 9.

$$1 = 9 - 2 \cdot 4$$

Therefore the Bézout coefficients of 9 and 4 are 1 and -2, respectively, and the coefficient of 4, namely -2, is the inverse.

b) $a = 19$, $m = 141$

First, we carry out the Euclidean algorithm to find $\gcd(19, 141)$:

$$141 = 7 \cdot 19 + 8$$
$$19 = 2 \cdot 8 + 3$$
$$8 = 2 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1$$

Then we work backwards to rewrite the gcd (the last nonzero remainder, which is 1 here) in terms of 19 and 141.

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (8 - 2 \cdot 3) = 3 \cdot 3 - 1 \cdot 8 \\ &= 3 \cdot (19 - 2 \cdot 8) - 1 \cdot 8 = 3 \cdot 19 - 7 \cdot 8 \\ &= 3 \cdot 19 - 7 \cdot (141 - 7 \cdot 19) = (-7) \cdot 141 + 52 \cdot 19 \end{aligned}$$

Therefore the Bézout Coefficients of 19 is 52, and that is an inverse of 19 modulo 141.

c) $a = 55$, $m = 89$

First, we carry out the Euclidean algorithm to find $\gcd(55, 89)$:

$$89 = 1 \cdot 55 + 34$$
$$55 = 1 \cdot 34 + 21$$
$$34 = 1 \cdot 21 + 13$$
$$21 = 1 \cdot 13 + 8$$
$$13 = 1 \cdot 8 + 5$$
$$8 = 1 \cdot 5 + 3$$
$$5 = 1 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1$$

Then we work backwards to rewrite the gcd (the last nonzero remainder, which is 1 here) in terms of 55 and 89.

$$1 = 3 - 1 \cdot 2$$

$$
\begin{aligned}
&= 3 - 1 \cdot (5 - 1 \cdot 3) = 2 \cdot 3 - 1 \cdot 5\\
&= 2 \cdot (8 - 1 \cdot 5) - 1 \cdot 5 = 2 \cdot 8 - 3 \cdot 5\\
&= 2 \cdot 8 - 3 \cdot (13 - 1 \cdot 8) = 5 \cdot 8 - 3 \cdot 13\\
&= 5 \cdot (21 - 1 \cdot 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13\\
&= 5 \cdot 21 - 8 \cdot (34 - 1 \cdot 21) = 13 \cdot 21 - 8 \cdot 34\\
&= 13 \cdot (55 - 1 \cdot 34) - 8 \cdot 34 = 13 \cdot 55 - 21 \cdot 34\\
&= 13 \cdot 55 - 21 \cdot (89 - 1 \cdot 55) = 34 \cdot 55 - 21 \cdot 89
\end{aligned}
$$

Therefore the Bézout coefficient of 55 is 34, which is an inverse of 55 modulo 89.

d) $a = 89$, $m = 232$
First, we carry out the Euclidean algorithm to find $\gcd(89, 232)$:

$$
\begin{aligned}
&232 = 2 \cdot 89 + 54\\
&89 = 1 \cdot 54 + 35\\
&54 = 1 \cdot 35 + 19\\
&35 = 1 \cdot 19 + 16\\
&19 = 1 \cdot 16 + 3\\
&16 = 5 \cdot 3 + 1\\
&3 = 3 \cdot 1
\end{aligned}
$$

Then we work backwards to rewrite the gcd (the last nonzero remainder, which is 1 here) in terms of 89 and 232.

$$
\begin{aligned}
1 &= 16 - 5 \cdot 3\\
&= 16 - 5 \cdot (19 - 1 \cdot 16) = 6 \cdot 16 - 5 \cdot 19\\
&= 6 \cdot (35 - 1 \cdot 19) - 5 \cdot 19 = 6 \cdot 35 - 11 \cdot 19\\
&= 6 \cdot 35 - 11 \cdot (54 - 1 \cdot 35) = 17 \cdot 35 - 11 \cdot 54\\
&= 17 \cdot (89 - 1 \cdot 54) - 11 \cdot 54 = 17 \cdot 89 - 28 \cdot 54\\
&= 17 \cdot 89 - 28 \cdot (232 - 2 \cdot 89) = 73 \cdot 89 - 28 \cdot 232
\end{aligned}
$$

Therefore the Bézout coefficient of 89 is 73, which is an inverse of 89 modulo 232.

6. Solve the congruence $4x \equiv 5 \pmod 9$ using the inverse of 4 modulo 9 found in part (a) of Exercise 5.

In Exercise 5a we found that an inverse of 4 modulo 9 is 7. Therefore we multiply both sides of this equation by 7:

$$7 \cdot 4x \equiv 5 \cdot 7 \pmod 9 \implies 28x \equiv 35 \pmod 9 \implies x \equiv 8 \pmod 9$$

And we can check our answer by computing:

$$4 \cdot 8 = 32 \equiv 5 \pmod 9$$

7. Solve each of these congruences using the modular inverses found in parts (b), (c), and (d) of Exercise 5.

a) $19x \equiv 4 \pmod{141}$
In Exercise 5b we found that an inverse of 19 modulo 141 is 52:

$$52 \cdot 19x \equiv 4 \cdot 52 \pmod{141} \implies 988x \equiv 208 \pmod{141} \implies x \equiv 67 \pmod{141}$$

Answer check: $19 \cdot 67 = 1273 \equiv 4 \pmod{141}$

b) $55x \equiv 34 \pmod{89}$

In Exercise 5c we found that an inverse of 55 modulo 89 is 34:

$$34 \cdot 55x \equiv 34 \cdot 34 \pmod{89} \implies 1870x \equiv 1156 \pmod{89} \implies x \equiv 88 \pmod{89}$$

Answer check: $55 \cdot 88 = 4840 \equiv 34 \pmod{89}$

c) $89x \equiv 2 \pmod{232}$

In Exercise 5d we found that an inverse of 89 modulo 232 is 73:

$$73 \cdot 89x \equiv 2 \cdot 73 \pmod{232} \implies 6497x \equiv 146 \pmod{232} \implies x \equiv 146 \pmod{232}$$

Answer check: $89 \cdot 146 = 12994 \equiv 2 \pmod{232}$

8. Use the Chinese remainder theorem to find all solutions to the system of congruences $x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, and $x \equiv 4 \pmod{11}$.

Since 2, 3, 5, and 11 are pairwise relatively prime, we can use the Chinese remainder theorem. We have a_1, $m_1 = 2$, $a_2 = 2$, $m_2 = 3$, $a_3 = 3$, $m_3 = 5$, $a_4 = 4$, $m_4 = 11$, $m = 330$, $M_1 = 330/2 = 165$, $M_2 = 330/3 = 110$, $M_3 = 330/5 = 66$, $M_4 = 330/11 = 30$. Then we need to find inverses y_i of M_i modulo m_i for $i = 1, 2, 3, 4$. We find that $y_1 = 1$, $y_2 = 2$, $y_3 = 1$, and $y_4 = 7$. Thus our solution is $x = 1 \cdot 165 \cdot 1 + 2 \cdot 110 \cdot 2 + 3 \cdot 66 \cdot 1 + 4 \cdot 30 \cdot 7 = 1643 \equiv 323 \pmod{330}$. So the solutions are all integers of the form $323 + 330k$, where k is an integer.

9. Write out in pseudocode an algorithm for solving a simultaneous system of linear congruences based on the Chinese remainder theorem.

```
procedure Chinese($m_1, m_2, \ldots, m_n$ : relatively prime positive integers; $a_1, a_2, \ldots, a_n$ : integers)
$m := 1$
for $k := 1$ to $n$
    $m := m \cdot m_k$
for $k := 1$ to $n$
    $M_k := m/m_k$
    $y_k := M_k^{-1}$ mod $m_k$ {use Euclidean algorithm or back-substitution to find inverse}
$x := 0$
for $k := 1$ to $n$
    $x := x + a_k M_k y_k$
while $x \geq m$
    $x := x - m$
return $x$ {the smallest solution to the system $\{x \equiv a_k \pmod{m_k}, k = 1, 2, \ldots, n\}$}
```

10. Use Fermat's little theorem to find 7^{121} mod 13.

Fermat's little theorem tells us that $7^{12} \equiv 1 \pmod{13}$. Note that $121 = 10 \cdot 12 + 1$. Therefore $7^{121} = 7^{12 \cdot 10} \cdot 7 = (7^{12})^{10} \cdot 7 \equiv 1^{10} \cdot 7 = 7 \pmod{13}$.

11. Use Fermat's little theorem to find 23^{1002} mod 41.

Fermat's little theorem tells us that $23^{40} \equiv 1 \pmod{41}$. Note that $1002 = 25 \cdot 40 + 2$. Therefore $23^{1002} = 23^{40 \cdot 25} \cdot 23^2 = (23^{40})^{25} \cdot 23^2 \equiv 1^{25} \cdot 23^2 = 529 = 37 \pmod{41}$.

12. Use Fermat's little theorem to show that if p is prime and $p \not| a$, then a^{p-2} is an inverse of a modulo p.

Fermat's little theorem tells us that under the given conditions $a^{p-1} \equiv 1 \pmod{p}$. Therefore $a^{p-2} \cdot a = a \cdot a^{p-2} = a^{p-1} \equiv 1 \pmod{p}$. This is precisely the definition that a^{p-2} is an inverse of a modulo p.

4.5 Applications of Congruences

1. Which memory locations are assigned by the hashing function $h(k) = k \bmod 97$ to the records of insurance company customers with these Social Security numbers?

a) $034567981 \bmod 97 = 91$

b) $183211232 \bmod 97 = 57$

c) $220195744 \bmod 97 = 21$

d) $987255335 \bmod 97 = 5$

2. A parking lot has 31 visitor spaces, numbered from 0 to 30. Visitors are assigned parking spaces using the hashing function $h(k) = k \bmod 31$, where k is the number formed from the first three digits on a visitor's license plate.

a) Which spaces are assigned by the hashing function to cars that have these first three digits on their license plates: 317, 918, 007, 100, 111, 310?
$h(317) = 317 \bmod 31 = 7$
$h(918) = 918 \bmod 31 = 19$
$h(007) = 007 \bmod 31 = 7$
$h(100) = 100 \bmod 31 = 7$
$h(111) = 111 \bmod 31 = 18$
$h(310) = 310 \bmod 31 = 0$

b) Describe a procedure visitors should follow to find a free parking space, when the space they are assigned is occupied.

They should take the next available space, where the next space is computed by adding, modulo 31, 1 to the space number.

3. A way to resolve collisions in hashing is to use *double hashing*. We use an initial hashing function $h(k) = k \bmod p$, where p is prime. We also use a second hashing function $g(k) = (k+1) \bmod (p-2)$. When a collision occurs, we use a *probing sequence* $h(k,i) = (h(k) + i \cdot g(k)) \bmod p$.

Use the double hashing procedure we have described with $p = 4969$ to assign memory locations to files for employees with social security numbers $k_1 = 132489971$, $k_2 = 509496993$, $k_3 = 546332190$, $k_4 = 034367980$, $k_5 = 047900151$, $k_6 = 329938157$, $k_7 = 212228844$, $k_8 = 325510778$, $k_9 = 353354519$, $k_{10} = 053708912$.

Initial hashes:

$h(132489971) = 132489971 \bmod 4969 = 1524$
$h(509496993) = 509496993 \bmod 4969 = 578$
$h(546332190) = 546332190 \bmod 4969 = 578$
$h(034367980) = 034367980 \bmod 4969 = 2376$
$h(047900151) = 047900151 \bmod 4969 = 3960$
$h(329938157) = 329938157 \bmod 4969 = 1526$
$h(212228844) = 212228844 \bmod 4969 = 2854$
$h(325510778) = 325510778 \bmod 4969 = 1526$
$h(353354519) = 353354519 \bmod 4969 = 3960$
$h(053708912) = 053708912 \bmod 4969 = 3960$

Collisions:

$578 : 509496993, 546332190$
$3960 : 47900151, 353354519, 53708912$
$1526 : 329938157, 325510778$

Probing sequences:

$h(509496993, 2) = (h(509496993 + 2 \cdot g(509496993)) \bmod 4969 = 4582$
$h(546332190, 3) = (h(546332190 + 3 \cdot g(546332190)) \bmod 4969 = 1390$
$h(47900151, 5) = (h(47900151 + 5 \cdot g(47900151)) \bmod 4969 = 939$
$h(353354519, 9) = (h(353354519 + 9 \cdot g(353354519)) \bmod 4969 = 3344$
$h(53708912, 10) = (h(53708912 + 10 \cdot g(53708912)) \bmod 4969 = 1442$
$h(329938157, 6) = (h(329938157 + 6 \cdot g(329938157)) \bmod 4969 = 2822$
$h(325510778, 8) = (h(325510778 + 8 \cdot g(325510778)) \bmod 4969 = 3889$

4. What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (3x_n + 2) \bmod 13$ with seed $x_0 = 1$?

$x_1 = (3 \cdot 1 + 2) \bmod 13 = 5$
$x_2 = (3 \cdot 5 + 2) \bmod 13 = 4$
$x_3 = (3 \cdot 4 + 2) \bmod 13 = 1$
$x_4 = (3 \cdot 1 + 2) \bmod 13 = 5$
$\ldots$

5. What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (4x_n + 1) \bmod 7$ with seed $x_0 = 3$?

$x_1 = (4 \cdot 3 + 1) \bmod 7 = 6$
$x_2 = (4 \cdot 6 + 1) \bmod 7 = 4$
$x_3 = (4 \cdot 4 + 1) \bmod 7 = 3$
$x_4 = (4 \cdot 3 + 1) \bmod 7 = 6$
$\ldots$

6. What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = 3x_n \bmod 11$ with seed $x_0 = 2$?

$x_1 = 3 \cdot 2 \bmod 11 = 6$
$x_2 = 3 \cdot 6 \bmod 11 = 7$
$x_3 = 3 \cdot 7 \bmod 11 = 10$
$x_4 = 3 \cdot 10 \bmod 11 = 8$
$x_5 = 3 \cdot 8 \bmod 11 = 2$
$x_6 = 3 \cdot 2 \bmod 11 = 6$
$\ldots$

7. The **power generator** is a method for generating pseudorandom numbers. To use the power generator, parameters p and d are specified, where p is prime, d is a positive integer such that p does not divide d, and a seed x_0 is specified. The pseudorandom numbers $x_1, x_2, \ldots$ are generated using the recursive definition $x_{n+1} = x_n^d \bmod p$.

a) Find the sequence of pseudorandom numbers generated by the power generator with $p = 7$, $d = 3$, and seed $x_0 = 2$.
$x_1 = 2^3 \bmod 7 = 1$
$x_2 = 1^3 \bmod 7 = 1$
$\ldots$

b) Find the sequence of pseudorandom numbers generated by the power generator with $p = 11$, $d = 2$, and seed $x_0 = 3$.
$x_1 = 3^2 \bmod 11 = 9$
$x_2 = 9^2 \bmod 11 = 4$
$x_3 = 4^2 \bmod 11 = 5$
$x_4 = 5^2 \bmod 11 = 3$
$x_5 = 3^2 \bmod 11 = 9$
$\ldots$

4.6 Cryptography

1. Encrypt the message DO NOT PASS GO by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.

a) $f(p) = (p+3) \bmod 26 \implies$ GR QRW SDVV JR
b) $f(p) = (p+13) \bmod 26 \implies$ QB ABG CNFF TB
c) $f(p) = (3p+7) \bmod 26 \implies$ QX UXM AHJJ ZX

2. Encrypt the message STOP POLLUTION by translating the letters into numbers, applying the given encryption, and then translating the numbers back into letters.

a) $f(p) = (p+4) \bmod 26 \implies$ WXST TSPPYXMSR
b) $f(p) = (p+21) \bmod 26 \implies$ NOJK KJGGPODJI
c) $f(p) = (17p+22) \bmod 26 \implies$ QHAR RABBYHCAJ

3. Encrypt the message WATCH YOUR STEP by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.

a) $f(p) = (p+14) \bmod 26 \implies$ KOHQV MCIF GHSD
b) $f(p) = (14p+21) \bmod 26 \implies$ RVBXP TJPZ NBZX
c) $f(p) = (-7p+1) \bmod 26 \implies$ DBYNE PHRM FYZA

4. Decrypt these messages that were encrypted using the Caesar cipher.

a) EOXH MHDQV $\implies$ BLUE JEANS
b) WHVW WRGDB $\implies$ TEST TODAY
c) HDW GLP VXP $\implies$ EAT DIM SUM

5. Decrypt these messages encrypted using the shift cipher $f(p) = (p+10) \bmod 26$.

a) CEBBOXNOB XYG $\implies$ SURRENDER NOW
b) LO WI PBSOXN $\implies$ BE MY FRIEND
c) DSWO PYB PEX $\implies$ TIME FOR FUN

6. Suppose that when a long string of text is encrypted using a shift cipher $f(p) = (p+k) \bmod 26$, the most common letter in the ciphertext is X. What is the most likely value for k, assuming that the distribution of letters in the text is typical of English text?

Since E is statistically the most commonly used letter in English text, we will assume that X represents E in the ciphertext. With E as 4 and X as 23 we can get k by finding their difference: $k = 23 - 4 = 19$.

7. Suppose that when a string of English text is encrypted using a shift cipher $f(p) = (p+k) \bmod 26$, the resulting ciphertext is DY CVOOZ ZOBMRKXMO DY NBOKW. What was the original plaintext string.

TO SLEEP PERCHANCE TO DREAM at $k = 10$.

8. Suppose that the ciphertext DVE CFMV KF NFEUVI, REU KYRK ZJ KYV JVVU FW JTZVETV was produced by encrypting a plaintext message using a shift cipher. What is the original plaintext?

MEN LOVE TO WONDER, AND THAT IS THE SEED OF SCIENCE at $k = 17$.

9. Suppose that the ciphertext ERC WYJJMGMIRXPC EHZERGIH XIGLRSPSKC MW MRHMWXMRKYMWLEFP JVSQ QEKMG was produced by encrypting a plaintex message using a shift cipher. What was the original plaintext?

ANY SUFFICIENTLY ADVANCED TECHNOLOGY IS INDISTINGUISHABLE FROM MAGIC at $k = 4$.

10. What is the decryption function for an affine cipher if the encryption function is $c = (15p + 13) \bmod 26$?

We want to solve the congruence $c \equiv 15p + 13 \pmod{26}$ for p. To do that we will need an inverse of 15 modulo 26, which is 7 (found using the extended Euclidean algorithm) because $7 \cdot 15 = 105 = 4 \cdot 26 + 1$. Therefore, we have $p = 7(c - 13) \bmod 26 = 7c - 91 \bmod 26 = 7c + 13 \bmod 26$.

11. Suppose that the most common letter and the second most common letter in a long ciphertext produced by encrypting plaintext using an affine cipher $f(p) = (ap + b) \bmod 26$ are Z and J, respectively. What are the most likely values of a and b?

Because the most common letters are E and T, in that order, and the numerical values of E, T, Z, and J are 4, 19, 25, and 9, respectively, we will assume that $f(4) \equiv 25$ and $f(19) \equiv 9$. This means that $4a + b \equiv 25$ and $19a + b \equiv 9$, where we work modulo 26. Subtracting the two equations gives $15a \equiv 10$, which simplifies to $3a \equiv 2$ (because 5 is not a factor of 26, we can divide both sides by 5). We can find an inverse of 3 modulo 26 using the Euclidean algorithm or trial and error. It is 9, because $3 \cdot 9 = 27 = 26 + 1$. Therefore $a \equiv 9 \cdot 2 = 18$. Plugging this into $4a + b \equiv 25$ yields $b \equiv 25 - 4a = 25 - 72 \equiv 5$. We therefore guess that the encryption function is $f(p) = 18p + 5 \bmod 26$. As a check, we see that $f(4) = 25$ and $f(19) = 9$.

12. Decrypt the message EABW EFRO ATMR ASIN, which is the ciphertext produced by encrypting a plaintext message using the transposition cipher with blocks of four letters and the permutation σ of $\{1, 2, 3, 4\}$ defined by $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$, and $\sigma(4) = 2$.

We permute each block of four by undoing the permutation σ. Because $\sigma(1) = 3$, we put the third letter first; because $\sigma(2) = 1$, we put the first letter second; and so on. This gives us BEWA REOF MART IANS, presumably meant to be BEWARE OF MARTIANS.

13. The ciphertext OIKYWVHBX was produced by encrypting a plaintext message using the Vigenére cipher with key HOT. What is the plaintext message?

The numerical version of the encrypted text is 14-8-10-24-22-21-7-1-23. If we subtract the values for the key HOTHOTHOT, namely 7-14-19-7-14-19-7-14-19 and reduce modulo 26, we obtain 7-20-17-17-8-2-0-13-4, which translates to HURRICANE.

14. Encrypt the message ATTACK using the RSA system with $n = 43 \cdot 59$ and $e = 13$, translating each letter into integers and grouping together pairs of integers.

The encrypted message is 0615 1576 2382.

15. Encrypt the message UPLOAD using the RSA system with $n = 53 \cdot 61$ and $e = 17$, translating each letter into integers and grouping together pairs of integers.

The encrypted message is 2545 2757 1211.

16. What is the original message encrypted using the RSA system with $n = 53 \cdot 61$ and $e = 17$ if the encrypted message is 3185 2038 2460 2550?

The original message is SQUIRREL.

17. What is the original message encrypted using the RSA system with $n = 43 \cdot 59$ and $e = 13$ if the encrypted message is 0667 1947 0671?

The original message is SILVER.