INSTRUCTOR'S SOLUTIONS MANUAL

INTRODUCTION TO CRYPTOGRAPHY WITH CODING THEORY

THIRD EDITION

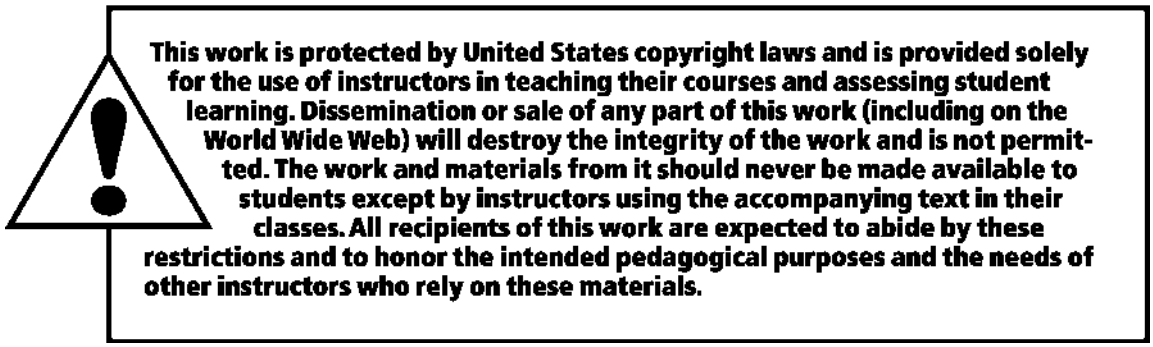
Wade Trappe

Rutgers University

Lawrence C. Washington

University of Maryland

Pearson



Reproduced by Pearson from electronic files supplied by the author.

ISBN-13: 978-0-13-487691-7
ISBN-10: 0-13-487691-1

Contents

Exercises

Mathematica problems

Maple problems

MATLAB problems

Sage problems

Chapter 2 - Exercises

1. Among the shifts of *EVIRE*, there are two words: *arena* and *river*. Therefore, Anthony cannot determine where to meet Caesar.

3. The inverse of 9 mod 26 is 3. Therefore, the decryption function is $x = 3(y-2) = 3y-6 \pmod{26}$. Now simply decrypt letter by letter as follows. $U = 20$ so decrypt U by calculating $3 * 20 - 6 \pmod{26} = 2$, and so on. The decrypted message is 'cat'.

5. Changing the plaintext to numbers yields 7, 14, 22, 0, 17, 4, 24, 14, 20. Applying $5x+7$ to each yields $5 \cdot 7+7 = 42 \equiv 16 \pmod{26}$, $5 \cdot 14+7 = 77 \equiv 25$, etc. Changing back to letters yields *QZNIIOBXZD* as the ciphertext. The decryption function is $21x + 9$.

7. Let $mx + n$ be the encryption function. Since $h = 7$ and $N = 13$, we have $m \cdot 7 + n \equiv 13 \pmod{26}$. Using the second letters yields $m \cdot 0 + n \equiv 14$. Therefore $n = 14$. The first congruence now yields $7m \equiv -1 \pmod{26}$. This yields $m = 11$. The encryption function is therefore $11x + 14$.

9. Let the decryption function be $x = ay + b$. The first letters tell us that $7 \equiv a \cdot 2 + b \pmod{26}$. The second letters tell us that $0 \equiv a \cdot 17 + b$.Subtracting yields $7 \equiv a \cdot (-15) \equiv 11a$. Since $11^{-1} \equiv 19 \pmod{26}$, we have $a \equiv 19 \cdot 7 \equiv 3 \pmod{26}$. The first congruence now tells us that $7 \equiv 3 \cdot 2 + b$, so $b = 1$. The decryption function is therefore $x \equiv 3y + 1$. Applying this to *CRWWZ* yields *happy* for the plaintext.

11. Let $mx + n$ be one affine function and $ax + b$ be another. Applying the first then the second yields the function $a(mx+n)+b = (am)x+(an+b)$, which is an affine function. Therefore, successively encrypting with two affine functions is the same as encrypting with a single affine function. There is therefore no advantage of doing double encryption in this case. (Technical point: Since $\gcd(a, 26) = 1$ and $\gcd(m, 26) = 1$, it follows that $\gcd(am, 26) = 1$, so the affine function we obtained is still of the required form.)

13. For an affine cipher $mx + n \pmod{27}$, we must have $\gcd(27, m) = 1$, and we can always take $1 \leq m \leq 27$. So we must exclude all multiples of 3, which leaves 18 possibilities for m. All 27 values of n are possible, so we have $18 \cdot 27 = 486$ keys. When we work mod 29, all values $1 \leq m \leq 28$ are allowed, so we have $28 \cdot 29 = 812$ keys.

15. (a) In order for α to be valid and lead to a decryption algorithm, we need $\gcd(\alpha, 30) = 1$. The possible values for α are $1, 7, 11, 13, 17, 19, 23, 29$.

(b) We need to find two x such that $10x \pmod{30}$ gives the same value.

There are many such possible answers, for example $x = 1$ and $x = 4$ will work. This corresponds to the letters 'b' and 'e'.

17. If $x_1 = x_2 + (26/d)$, then $\alpha x_1 + \beta = \alpha x_2 + \beta + (\alpha/d)26$. Since $d = \gcd(\alpha, 26)$ divides α, the number $\alpha/26$ is an integer. Therefore $(\alpha/d)26$ is a multiple of 26, which means that $\alpha x_1 + \beta \equiv \alpha x_2 + \beta \pmod{26}$. Therefore x_1 and x_2 encrypt to the same ciphertext, so unique decryption is impossible.

19. (a) In order to find the most probable key length, we write the ciphertext down on two strips and shift the second strip by varying amounts. The shift with the most matches is the most likely key length. As an example, look at the shift by 1:

```
B  A  B  A  B  A  A  A  B  A
   B  A  B  A  B  A  A  A  B  A
               *  *
```

This has a total of 2 matches. A shift by 2 has 6 matches, while a shift by 3 has 2 matches. Thus, the most likely key length is 2.

(b) To decrypt, we use the fact that the key length is 2 and extract off every odd letter to get BBBAB, and then every even letter to get AAAAA. Using a frequency count on each of these yields that a shift of 0 is the most likely scenario for the first character of the Vigenere key, while a shift of 1 is the most likely case for the second character of the key. Thus, the key is *AB*. Decrypting each subsequence yields BBBAB and BBBBB. Combining them gives the original plaintext BBBBBBABBB.

21. If we look at shifts of 1, 2, and 3 we have 2, 3, and 1 matches. This certainly rules out 3 as the key length, but the key length may be 1 or 2.

In the ciphertext, there are 3 *A*'s, 5 *B*'s, and 2 *C*'s. If the key length were 1, this should approximate the frequencies .7, .2, .1 of the plaintext in some order, which is not the case. So we rule out 1 as the key length.

Let's consider a key length of 2. The first, third, fifth, ... letters are *ACABA*. There are 3 *A*'s, 1 *B*, and 1*C*. These frequencies of .6, .2, .2 is a close match to .7, .2, .1 shifted by 0 positions. The first element of the key is probably *A*. The second, fourth, ... letters of the ciphertext are *BBBBC*. There are 0 *A*'s, 4 *B*'s, and 1 *C*. These frequencies .0, .8, .2 and match .7, .2, .1 with a shift by 1. Therefore the second key element is probably *B*.

Since the results for length 2 match the frequencies most closely, we conclude that the key is probably *AB*.

23. Since the entries of $\mathbb{A}_i$ are the same as those in $\mathbb{A}_0$ (shifted a few places) the two vectors have the same length. Therefore

$$\mathbb{A}_0 \cdot \mathbb{A}_i = |\mathbb{A}_0||\mathbb{A}_i| \cos\theta = |\mathbb{A}_0|^2 \cos\theta.$$

Note that $\cos\theta \leq 1$, and equals 1 exactly when $\theta = 0$. But $\theta = 0$ exactly when the two vectors are equal. So we see that the largest value of the cosine is when $\mathbb{A}_0 = \mathbb{A}_i$. Therefore the largest value of the dot product is when $i = 0$.

25. (a) The ciphertext will be one letter repeated a few hundred times, so the plaintext must also be a repeated letter. But the plaintext could be the shift of any letter, so the key and the plaintext cannot be deduced.

(b) The ciphertext will be one letter repeated a few hundred times, so the plaintext must also be a repeated letter. But the plaintext could be the encryption of any letter, so the key and the plaintext cannot be deduced.
(c) The ciphertext will be a sequence of letters repeated many times. This means that the plaintext consists of a pattern of letters that is repeated (for example, if the key length is 6, then three letters repeated many times would cause the ciphertext to repeat every 6 letters). If the key is a word, then the ciphertext is this word repeated several times. But Eve cannot be sure of this, so the key and the plaintext cannot be deduced with certainty.

27. EK IO IR NO AN HF YG BZ YB LF GM ZN AG ND OD VC MK

29. AAXFFGDGAFAX

31. (a) Since $2^{128} = 2^{64} \cdot 2^{64}$, it will take 2^{64} days, which is approximately 5×10^{16} years.
(b) It will take around 5×10^{14} years (the offset by 10 years is insignificant), which is much less that the time in part (a).

Chapter 3 - Exercises

1. (a) Apply the Euclidean algorithm to 17 and 101:

$$101 = 5 \cdot 17 + 16$$

$$17 = 1 \cdot 16 + 1.$$

Working back yields $1 = 17 - 16 = 17 - (101 - 5 \cdot 17) = (-1) \cdot 101 + 6 \cdot 17$.

(b) Since $-101+6 \cdot 17 = 1$, we have $6 \cdot 17 \equiv 1 \pmod{101}$. Therefore $17^{-1} \equiv 6 \pmod{101}$.

3. (a) Apply the Euclidean algorithm to 7 and 30:

$$30 = 4 \cdot 7 + 2$$

$$7 = 3 \cdot 2 + 1.$$

Working backwards yields $1 = 7 - 3 \cdot 2 = 7 - 3 \cdot (30 - 4 \cdot 7) = 13 \cdot 7 + (-3) \cdot 30$. Therefore $13 \cdot 7 \equiv 1 \pmod{30}$, so $d = 13$.

(b) Let $c \equiv m^7 \pmod{31}$ be the ciphertext. Claim: $c^{13} \equiv m \pmod{31}$. Proof: $c^13 \equiv (m^7)^{13} = m^{91} \equiv (m^{30})^3 m$. If $m \not\equiv 0 \pmod{31}$ then $m^{30} \equiv 1 \pmod{31}$ by Fermat. Then $c^{13} \equiv 1^3 m \equiv m$. If $m \equiv 0 \pmod{31}$, then $c \equiv m^7 \equiv 0$, so $c^{13} \equiv 0^{13} \equiv 0 \equiv m$. Therefore $c^{13} \equiv m$ for all m. Therefore decryption is performed by raising the ciphertext to the 13th power mod 31.

5. (a) $\gcd(12, 236) = 4$, so divide both sides by 4 to obtain $3x \equiv 7 \pmod{59}$. The inverse of 3 mod 59 is 20, so multiply both sides by 20 to obtain $x \equiv 140 \equiv 22 \pmod{59}$. This yields $x \equiv 22, 81, 140, 199 \pmod{236}$.
(b) 30 is not divisible by $4 = \gcd(12, 236)$, so there are no solutions.

7. (a) Since n is composite, we can write $n = ab$, with $a, b \geq 2$. If $a > \sqrt{n}$ and $b > \sqrt{n}$, then $n = ab > \sqrt{n}\sqrt{n} = n$, which is impossible. Therefore, either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. Let's say it's a. Let p be a prime factor of a. Then $p \leq a \leq \sqrt{n}$, as desited.

(b)

$$\begin{aligned} 30030 &= 116 \cdot 257 + 218 \\ 257 &= 1 \cdot 218 + 39 \\ 218 &= 5 \cdot 39 + 23 \\ 39 &= 1 \cdot 23 + 16 \\ 23 &= 1 \cdot 16 + 7 \\ 16 &= 2 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Therefore, $\gcd(30030, 257) = 1$.
(c) If 257 is composite, it is divisible by a prime $p \leq \sqrt{257} = 16.03\ldots$. The primes satisfying this are exactly the prime factors of 30030. Since the gcd is 1, none of them divide 257, so 257 is prime.

9. (a)

$$\begin{aligned} 4883 &= 1 \cdot 4369 + 514 \\ 4369 &= 8514 + 257 \\ 514 &= 2 \cdot 257 + 0. \end{aligned}$$

Therefore, the gcd is 257.
(b) We know that both numbers have 257 as a factor. This yields $4883 = 257 \cdot 19$ and $4369 = 257 \cdot 17$.

11. (a) The first two steps of the Euclidean algorithm are

$$\begin{aligned} F_n &= 1 \cdot F_{n-1} + F_{n-2} \\ F_{n-1} &= 1 \cdot F_{n-2} + F_{n-3}. \end{aligned}$$

It continues in this way until

$$\begin{aligned} 2 &= 2 \cdot 1 + 1 \\ 1 &= 1 \cdot 1 + 0. \end{aligned}$$

Therefore, the gcd is 1.
(b)

$$\begin{aligned} 11111111 &= 1000 \cdot 11111 + 111 \\ 11111 &= 100 \cdot 111 + 11 \\ 111 &= 10 \cdot 11 + 1 \\ 11 &= 11 \cdot 1 + 0. \end{aligned}$$

Therefore, the gcd is 1.
(c) The first step of the Euclidean algorithm is

$$a = 10^{F_{n-2}} \cdot b + c,$$

where c consists of F_{n-2} repeated 1's. Continuing in this way, in each step we divide F_{j-1} repeated 1's into F_j repeated 1's and get a remainder consisting of F_{j-2} repeated 1's. Eventually, we get down to the computations of part (b), and then obtain that the gcd is 1.

13. (a) If $ab \equiv 0 \pmod{p}$, then $p|ab$. By the Lemma in Subsection 3.1.2, since p is prime, either $p|a$ or $p|b$. Therefore, either $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

(b) We follow the proof of the Lemma in Subsection 3.1.2. Since $\gcd(a, n) = 1$, there are integers x, y such that $ax + ny = 1$. Multiply by b to obtain $abx + bny = b$. Since $n|ab$, both terms on the left are multiples of n. Therefore $n|b$.

15. $(x + 1)(x - 1) \equiv 0 \pmod{p}$ implies, by 3(a), that either $x + 1 \equiv 0 \pmod{p}$ or $x - 1 \equiv 0 \pmod{p}$. Therefore $x \equiv \pm 1 \pmod{p}$.

17. One solution is to look at the numbers congruent to 3 (mod 10) until we find one that is 2 (mod 7): $3,\ 13 \equiv 6,\ 23 \equiv 2 \pmod{7}$. Therefore $x \equiv 23 \pmod{70}$.

19. Suppose there are x people. Then $x \equiv 1 \pmod{3}, x \equiv 2 \pmod{4}, x \equiv 3 \pmod{5}$. The last two congruences combine to $x \equiv 18 \pmod{20}$. List the numbers that are 18 (mod 20) until you find one that is 1 (mod 3). The answer is $x \equiv 58 \pmod{60}$. The smallest number is 58 and the next smallest number is 118.

21. (a) Look at the congruence mod 11 and mod 13. We have $x^2 \equiv 133 \equiv 1 \pmod{11}$, which has solutions $x \equiv \pm 1 \pmod{11}$. We have $x^2 \equiv 133 \equiv 3 \pmod{13}$, which has solutions $x \equiv \pm 4 \pmod{13}$. There are four ways to combine these: For example, $x \equiv +1 \pmod{11}$ and $x \equiv +4 \pmod{13}$ combine to yield $x \equiv 56 \pmod{143}$. The other solutions are $x \equiv 43 \pmod{143}$, $x \equiv 100 \pmod{143}$, and $x \equiv 87 \pmod{143}$.

23. By Fermat's theorem, $2^{100} \equiv 1 \pmod{101}$. Therefore, $2^{10203} \equiv (2^{100})^{102}2^3 \equiv 1^{102}2^3 \equiv 8$. Therefore, the remainder is 8.

25. "Last two digits" means we work mod 100. Since $\phi(100) = 40$, Euler's theorem says that $123^{40} \equiv 1 \pmod{100}$. Therefore, $123^{562} \equiv (123^{40})^{14}123^2 \equiv 123^2 \equiv 23^2 \equiv 529 \equiv 29$. The last two digits are 29.

27. If $a \not\equiv 0 \pmod{p}$, then Fermat says that $a^{p-1} \equiv 1 \pmod{p}$. Multiply by a to get $a^p \equiv a \pmod{p}$. If $a \equiv 0 \pmod{p}$, then $a^p \equiv 0^p \equiv 0 \equiv a \pmod{}$. Therefore $a^p \equiv a \pmod{p}$ for all a.

29. (a) $7^7 \equiv (-1)^7 \equiv -1 \equiv 3 \pmod{4}$.

(b) $7^7 = 3 + 4k$ for some k. By Euler's theorem, $7^4 \equiv 1 \pmod{10}$. Therefore,

$$7^{7^7} \equiv 7^3(7^4)^k \equiv 7^3 \cdot 1^k \equiv 343 \equiv 3 \pmod{10}.$$

The last digit is 3.

31. (a) Since $p \nmid a$, Fermat says that $a^{p-1} \equiv 1 \pmod{p}$. For $p = 7$, we have $a^6 \equiv 1 \pmod{7}$, so $a^{1728} \equiv (a^6)^{288} \equiv 1^{288} \equiv 1 \pmod{7}$. Since $1728 = 12 \cdot 144$ and $1728 = 18 \cdot 96$, a similar argument works for $p = 13$ and for $p = 19$.

(b) If $p \nmid a$, then multiply the result of (a) by a to get $a^{1729} \equiv a \pmod{p}$. If $p|a$, then a^{1729} and a are both 0 (mod p), so $a^{1729} \equiv a$ in this case, too.

(c) Fix a number a. The Chinese Remainder Theorem says that $x \equiv a^{1729} \pmod 7, x \equiv a^{1729} \pmod{13}, x \equiv a^{1729} \pmod{19}$ has a unique solution $x \pmod{1729}$, since $1729 = 7 \cdot 13 \cdot 19$. We know two such solutions: $x = a$ (from part (b) and $x = a^{1729}$ (trivially). Since x is unique mod 1729, we must have $a \equiv a^{1729} \pmod{1729}$.

33. (a) $a \cdot b \equiv a \cdot a^{p-2} \equiv a^{p-1} \equiv 1 \pmod p$ by Fermat's theorem.
(b) Let $a = 2$. Then $b \equiv 2^5 \equiv 4 \pmod 7$. Multiply both sides of $2x \equiv 1$ by 4 to get $8x \equiv 4$, which says $x \equiv 4 \pmod 7$.

35. (a) $\phi(1) = 1, \phi(2) = 1, \phi(5) = 4, \phi(10) = 4$. The sum is 10.
(b) $\phi(1) = 1, \phi(2) = 1, \phi(3)2, \phi(4) = 2, \phi(6) = 2, \phi(12) = 4$. The sum is 12.
(c) The sum of $\phi(d)$, for all of the divisors d of n, equals n.

37. (a) The powers of 2 mod 11 are $2, 4, 8, 5, 10, 9, 7, 3, 6, 1$. This gives all nonzero congruence classes mod 11, so 2 is a primitive root mod 11.
(b) The inverse of 3 (mod 10) is 7. We obtain

$$8^7 \equiv (2^3)^7 \equiv 2^{21} \equiv (2^{10} \cdot 2^1 \equiv 1 \cdot 2 \equiv 2 \pmod{11}.$$

Therefore, $x = 7$.
(c) This can be done directly, but here is another way. If $c \not\equiv 0 \pmod{11}$, then $c \equiv 2^j$ for some j. Therefore, $c \equiv (8^7)^j \equiv 8^{7j} \pmod{11}$, so c is a power of 8.
(d) Write $xy = 1 + (p-1)k$. Then

$$h^x \equiv (g^y)^x \equiv g \cdot (g^{p-1})^k \equiv g \cdot 1^k \equiv g \pmod p.$$

(e) Let c be nonzero mod p. Then $c \equiv g^j \pmod p$ for some j, so $c \equiv (h^x)^j \equiv h^{xj} \pmod p$. Since every nonzero congruence class is a power of h, we have that h is a primitive root mod p.
(f) The numbers y with $1 \le y < p-1$ satisfying $\gcd(y, p-1) = 1$ are $1, 5, 7, 11$. Part (e) says that 2^y is a primitive root mod 13 for each of these values of y. Therefore, $2, 2^5 \equiv 6, 2^7 \equiv 11, 2^{11} \equiv 7$ are the primitive roots mod 13.

39. (a) The determinant is $1 \cdot 1 - 1 \cdot 6 = -5 \equiv 21 \pmod{26}$. The inverse of the determinant is 5 (mod 26). The inverse of the matrix is therefore

$$\frac{1}{21}\begin{pmatrix} 1 & -1 \\ -6 & 1 \end{pmatrix} \equiv 5\begin{pmatrix} 1 & -1 \\ -6 & 1 \end{pmatrix} \equiv \begin{pmatrix} 5 & 21 \\ 22 & 5 \end{pmatrix}.$$

(b) The determinant is $1 - b$. The matrix is invertible mod 26 exactly when $\gcd(1-b, 26) = 1$. This happens when $1 - b$ is odd and not 0 mod 13, so $b \equiv 0, 2, 4, 6, 8, 10, 12, 16, 18, 20, 22, 24 \pmod{26}$.

41. The determinant is $9 - 35 = -26$. This is divisible by 2 and by 13, so these are the two primes for which the matrix is not invertible mod p.

43. (a)

$$\left(\frac{123}{401}\right) = \left(\frac{401}{123}\right) = \left(\frac{32}{123}\right) = \left(\frac{2}{123}\right)^5 = -1.$$

Therefore, there is no solution.
(b)

$$\left(\frac{43}{179}\right) = -\left(\frac{179}{43}\right) = -\left(\frac{7}{43}\right) = \left(\frac{43}{7}\right) = \left(\frac{1}{43}\right) = 1.$$

Therefore, there is a solution.
(c)

$$\left(\frac{1093}{65537}\right) = \left(\frac{65537}{1093}\right) = \left(\frac{2}{1093}\right)\left(\frac{525}{1093}\right) = -\left(\frac{43}{525}\right) = -\left(\frac{9}{43}\right) = -1.$$

Therefore, there is no solution.

45. $\left(\frac{2}{15}\right) = 1$, but $2^7 \equiv 8 \pmod{15}$.

47. (a) The only polynomials of degree 1 are X and $X+1$, and they are irreducible. The only polynomials of degree 2 are $X^2, X^2+1, X^2+X, X^2+X+1$. But X^2 and $X^2+1 \equiv (X+1)^2$ are reducible, and so is $X^2+X \equiv X(X+1)$. Only X^2+X+1 remains. If it factors, it must be divisible by a degree one polynomial. Clearly X does not divide it. A simple calculation shows that $X+1$ does not divide it either. Therefore X^2+X+1 is irreducible.
(b) If X^4+X+1 factors, it must have an irreducible factor of degree at most 2. Since none of the polynomials from part (a) divide it, it must be irreducible.
(c) $X^4 \equiv -(X+1) \equiv X+1$, since we are working with coefficients mod 2. Square both sides to obtain $X^8 \equiv (X+1)^2 \equiv X^2+1$. Square again to obtain $X^{16} \equiv (X^2+1)^2 \equiv X^4+1 \equiv (X+1)+1 \equiv X$.
(d) Since X^4+X+1 is irreducible, polynomials mod X^4+X+1 form a field. Since $X \not\equiv 0 \pmod{X^4+X+1}$, it has a multiplicative inverse. Therefore, we can divide $X^{16} \equiv X$ by X to obtain $X^{15} \equiv 1$.

49. $a = q_1 b + r_1$ with $0 \le r_1 < b$. This means that

$$\frac{a}{b} = q_1 + \frac{r_1}{b}$$

with $0 \le r_1/b < 1$. Therefore, $a_0 = q_1$. Similarly, at each step of the algorithm, in the notation of Subsection 3.1.3, we have

$$\frac{r_{j-2}}{r_{j-1}} = q_j + \frac{r_j}{r_{j-1}},$$

which yields $a_{j-1} = q_j$.

51. Use a decimal approximation for e to obtain

$$a_0, a_1, a_2, a_3, \cdots = 2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, 1, 1, 14, \ldots.$$

After the initial 2, we get blocks of $1, 2n, 1$ for $n = 1, 2, 3, \ldots$.

53. (a) We know $a^{\phi(n)} \equiv 1 \pmod{n}$, by Euler. Since r is smallest, $r \le \phi(n)$.
(b) Since $a^r \equiv 1$, we have $a^m \equiv (a^r)^k \equiv 1^k \equiv 1 \pmod{n}$.
(c) By (b), $a^{qr} \equiv 1$. Therefore, $1 \equiv$ (by assumption)$a^t \equiv a^{qr}a^s \equiv 1 \cdot a^s \equiv a^s$.
(d) Since $a^s \equiv 1$ and r is the smallest positive integer with $a^r \equiv 1$, we must have $s = 0$. Therefore $t = qr$, so $r|t$.
(e) By Euler, $a^{\phi(n)} \equiv 1 \pmod{n}$. From part (d) with $t = \phi(n)$, we obtain $\mathrm{ord}_n(a)|\phi(n)$.

55. (a) We have $3^{16k} \equiv 2^k \not\equiv 1 \pmod{65537}$ and $3^{32k} \equiv 2^{32} \equiv 1 \pmod{65537}$. Therefore $65536 \nmid 16k$ and $65536|32k$. Write $32k = 65536\ell$ for some ℓ. Divide

by 32 to obtain $k = 2048\ell$, so $2^{11} = 2048|k$. If $2^{12} = 4096|k$, then $16k$ is a multiple of $16 \cdot 4096 = 65536$, which we showed doesn't happen. Therefore k is a multiple of 2048, but is not a multiple of 4096.

(b) From (a), we see that k is an odd multiple of 2048. We also know that $0 \le k < 65536$, since every nonzero number mod 65537 can be written as a power of 3 with exponent in this range. There are 65536/2048=32 multiples of 2048 in this range. Of these, 16 are multiples of 4096. The remaining 16 are possibilities for k. We now calculate $3^{2048m} \pmod{65537}$ for $m = 1, 3, 5, \cdots$. We find (with the help of a computer) that $m = 27$ works. So $k = 2048*27 = 55296$.

57. Note that when $j \neq i$, we have $z_j \equiv 0 \pmod{m_i}$ because z_j contains m_i as a factor. Therefore, $x \equiv 0 + \cdots + a_i y_i z_i + \cdots + 0 \equiv a_i y_i z_i \equiv a_i \pmod{m_i}$, since $y_i z_i \equiv 1 \pmod{m_i}$.

59. (a) Since $r_1 = a - bq_1$ and $d|a, b$, we have $d|r_1$. Since $r_2 = b - q_2 r_1$ and $d|b, r_1$, we have $d|r_2$.

(b) Suppose $d|r_1, \ldots, r_j$. Since $r_{j+1} = r_{j-1} - q_{j+1} r_j$ and $d|rj - 1, r_j$, we have $d|r_{j+1}$. By induction, we have $d|r_i$ for all i.

(c) Since $r_{k-1} = q_{k+1} r_k$, we have $r_k|r_{k-1}$. Assume $r_k|r_{k-i}$ for $i = 1, 2, \ldots, j$. Since $r_{k-j-1} = q_{k-j+1} r_{k-j} + r_{k-j+1}$ and $r_k|r_{k-j}, r_{k-j+1}$ by assumption, we have $r_k|r_{k-j-1}$. By induction, $r_k|r_i$ for all i.

(d) Since $b = q_2 r_1 + r_2$ and $r_k|r_1, r_2$, we have $r_k|b$. Since $a = q_1 b + r_1$ and $r_k|a, r_1$, we have $r|a$.

(e) Since $d|r_k$ for each common divisor d, we have $r_k \ge d$ for all common divisors d. Since r_k is a common divisor, it is the largest.

61. (a) $x \equiv 1 \pmod 4$, $x \equiv 2 \pmod 6$ has no solution.

(b) $x \equiv 2 \pmod 4$, $x \equiv 4 \pmod 6$ has the solution $x = 10$ (in fact, $x \equiv 10 \pmod{12}$ gives all solutions).