1. Chapter 1

1.1.3. If \( a \mid b \) and \( b \mid c \) show that \( a \mid c \).

Solution: \( a \mid b \) means that \( b = na \) and \( b \mid c \) that \( c = mb \). Substituting \( b = na \) gives \( c = (mn)a \), that is, \( a \mid c \).

1.2.1. Find an integer solution of \( 305x + 145y = \gcd(305,145) \).

Solution:

\[
egin{align*}
305 &= 2 \cdot 145 + 15 \\
145 &= 10 \cdot 15 - 5 \\
15 &= 3 \cdot 5 + 0
\end{align*}
\]

Hence \( 5 = \gcd(305,145) \) and substituting \( 15 = 305 - 2 \cdot 145 \) into the second equation gives

\[
5 = 10 \cdot 305 - 21 \cdot 145.
\]

When dividing 145 by 15 we have used a smaller reminder \(-5\) then the customary 10, to accelerate the process.

1.2.5. Let \( a \) and \( b \) be two integers. Show that any common divisor of \( a \) and \( b \) divides the greatest common divisor of \( a \) and \( b \).

Solution: Let \( d \) be the greatest common divisor. Then \( d = ax + by \) for some integers \( x \) and \( y \). Let \( c \) be a common divisor of \( a \) and \( b \). Then \( a = cm \) and \( b = cn \) for some integers \( n \) and \( m \). Substituting gives \( d = cmx + cny = c(mx + ny) \) i.e. \( c \) is a divisor of \( d \).

2. Chapter 2

2.1.1. Let \( G \) be a group and \( e \) and \( e' \) two identity elements. Show that \( e = e' \). Hint: consider \( e \circ e' \).

Solution: \( e \circ e' = e' \), since \( e \) is an identity element. \( e \circ e' = e' \) since \( e' \) is an identity element. Hence \( e = e' \).

2.1.3. Let \( G \) be a group. Assume that \( a = a^{-1} \) for every \( a \) in \( G \). Show that \( G \) is commutative, i.e. \( ab = ba \) for all \( a \) and \( b \) in \( G \).

Solution: \( ab = (ab)^{-1} = b^{-1}a^{-1} = ba \).

2.2.1. Prove that an integer is divisible by 11 if and only if the sum of its digits is divisible by 11.
Solution: Since $10 \equiv -1 \pmod{11}$, $10^k \equiv (-1)^k \pmod{9}$ for all integers $k \geq 0$. If $a_m, \ldots, a_0$ are decimal digits of an integer $n$, then

$$n = a_m10^m + \cdots + a_210^2 + a_110 + a_0 \equiv (-1)^m a_m + \cdots + a_2 - a_1 + a_0 \pmod{11}.$$ 

2.4.1. Let $G$ be a group and $g$ an element in $G$ of order $n$. Let $m$ be a positive integer such that $g^m = e$. Show that $n$ divides $m$.

Solution: Write $m = nq + r$ where $0 \leq r < n$. We want to show that $r = 0$. In addition to $g^m = e$, we also have $g^n = e$ since the order of $g$ is $n$. Then we have the following identities.

$$e = g^m = g^{nq + r} = (g^n)^e \cdot g^r = g^r.$$ 

Hence $g^r = e$ and this is possible only if $r = 0$.

2.4.5. Let $G$ be a group and $g$ an element in $G$ of order 9. What is the order of $g^3$? What is the order of $g^2$? Justify your answers.

Solution: Since the order of $g$ is 9, $g^9, g^{18}, g^{27}, g^{36}, \ldots$ are all powers of $g$ equal to the identity element in $G$. Thus the order of $g^k$ is the smallest integer $m$ such that $km$ is a multiple of 9. If $k = 3$ then $m = 3$, if $k = 2$ then $m = 9$.

2.4.7 Let $g$ be a group element such that $g^9 = e$ and $g^{16} = e$ where $e$ is the identity element. Show that $g = e$.

Solution: Since 9 and 16 are relatively prime there exist integers $x$ and $y$ such that $1 = 9x + 16y$. Then

$$g = g^1 = g^{9x + 16y} = g^{9x} \cdot g^{16y} = (g^9)^x \cdot (g^{16})^y = e \cdot e = e.$$ 

In a pedestrian way, $g^{16} = e$ and $g^9 = e$ imply that $g^7 = e$, then $g^9 = e$ and $g^7 = e$ imply that $g^2 = e$ etc.

2.5.3 Solve the system of congruences

$$x \equiv 4 \pmod{55}$$
$$x \equiv 11 \pmod{69}$$

Solution: The first equation implies $x = 4 + k \cdot 55$. Substituting into the second equation gives $k \cdot 55 = 7 \pmod{69}$. The inverse of 55 modulo 69 is $-5$. Thus $k = -35$.

2.5.5. Solve the system of congruences

$$x \equiv 11 \pmod{16}$$
$$x \equiv 16 \pmod{27}$$

Solution: The second equation implies $x = 16 + k \cdot 27$. Substituting into the first equation gives $k \cdot 11 = 11 \pmod{16}$, since $16 \equiv 0 \pmod{16}$ and $27 \equiv 11 \pmod{16}$, hence $k = 1$. Thus $x = 43$.

2.5.6. Find the last two digits of $3^{125}$.
Solution: The question is: What is $3^{101} \mod 100$? Since 3 is relatively prime to 100, we can use Euler’s theorem modulo 100. Since $\varphi(100) = \varphi(4) \varphi(25) = 2 \cdot 20 = 40$, it follows that $3^{40} \equiv 1 \mod 100$ and

$$3^{125} = 3^{3 \cdot 40 + 5} \equiv 3^5 = 43 \mod 100.$$ 

2.5.9. Compute $3^{25} \mod 45$. Hint: compute $3^{25} \mod 9$ and 5, then use CRT.

Solution: It is clear that $3^{45} \equiv 0 \mod 9$. Since $\varphi(5) = 4$, and 3 is prime to 5,

$$3^{25} \equiv 3 \mod 5.$$ 

Hence, we are looking for $x$ such that $3 + 5x \equiv 0 \mod 9$. The multiplicative inverse of 5 modulo 9 is 2, hence

$$x \equiv 2 \cdot (-3) \equiv 3 \mod 9.$$ 

The answer is $3 + 5 \cdot 3 = 18$.

3. Chapter 3

3.1.5. Let $R$ be a ring and let $-1$ denote the inverse of 1 for addition. Show that, for every $r \in R$, $(-1) \cdot r = -r$, where $-r$ is the inverse of $r$ for addition. Hint: use $r \cdot 0 = 0$.

Solution: Multiply $(1 + (-1)) = 0$ by $r$, use $r \cdot 0 = 0$ on the right, and the distributive property on the left to conclude that $r + (-1) \cdot r = 0$. Uniqueness of the additive inverse implies that $(-1) \cdot r$ is the additive inverse of $r$.

3.3.1. Find the inverse of $2 + 5i$ modulo 31. Is there an inverse of $2 + 5i$ modulo 29?

Solution: We are looking for $x + yi$ such that $(2 + 5i)(x + yi) = 1$. This leads to a pair of linear equations $2x - 5y = 1$ and $5x + 2y = 0$. Modulo 31 there is a unique solution, $x = 2/29$ and $y = -5/29$. The inverse of 29 modulo 31 is 15, so $30 + 18i$ is the inverse modulo 31. Modulo 29 the system has no solution: the determinant of the system is 29 $\equiv 0 \mod 29$, so the two lines are parallel, but they do not coincide, since $(0, 0)$ is a solution to only one of the two equations. Alternatively, observe that $(2 + 5i)/(2 - 5i) \equiv 0 \mod 29$, so $2 + 5i$ is a zero divisor, and thus it cannot be invertible.

4. Chapter 4

4.1.1. Let $S = \{p_1, \ldots, p_n\}$ be any list of odd primes. Let $m = 3p_1 \cdots p_n + 2$. Show that $m$ is divisible by an odd prime $q \equiv 2 \mod 3$ not in the set $S$. Conclude that there are infinitely many primes congruent to 2 modulo 3.

Solution: Let $m = q_1 \cdot q_2 \cdots q_s$ be a factorization into primes. Since $m$ is odd and not divisible by 3 none of the primes factors is 2 or 3. If $q_1 \equiv 1 \mod 3$ for all $i$ then $m \equiv 1 \mod 3$. But $m \equiv 2 \mod 3$, thus $q_i \equiv 2 \mod 3$ for at least one prime $q_i$.

5. Chapter 5

5.1.1 a) Solve $x^5 \equiv 2 \mod 35$.

Solution. The solution is $x \equiv 2^u \mod 35$ where $u$ is the inverse of 5 modulo 24 = $\varphi(35)$. Since $5 \cdot 5 \equiv 1 \mod 24$ the inverse of 5 if 5. Hence $x = 2^5 = 32$. 

5.1.1 d) Solve the congruence

\[ x^5 \equiv 3 \pmod{64}. \]

Solution: This is solved by taking both sides to the power \( a \), where \( a \) is the inverse of 5 modulo \( \varphi(64) = 32 \). Then the right side is \( x \) and the left hand side of the congruence is the solution \( 3^a \). The inverse of 5 is 13. It remains to compute \( 3^{13} \), and this is done by consecutive squaring: \( 3^4 \equiv 17 \pmod{64} \), \( 3^8 \equiv 33 \pmod{64} \). Hence

\[ 3^{13} = 3^8 \cdot 3^4 \cdot 3 \equiv 33 \cdot 17 \cdot 3 \equiv 19 \pmod{64}. \]

5.2.1. Let \( n = p^m \), where \( p \) is prime. Verify, by computing all terms in the sum, that

\[ \sum_{d|n} \varphi(d) = n. \]

Solution: The divisors of \( p^m \) are \( p^i \) where \( i = 0, 1, \ldots, m \). Since \( \varphi(1) = 1 \), and \( \varphi(p^i) = p^i - p^{i-1} \) for \( i > 0 \)

\[ \sum_{d|n} \varphi(d) = \sum_{i=1}^{m} \varphi(p^i) = 1 + (p - 1) + (p^2 - p) + \ldots + (p^m - p^{m-1}) = p^m = n. \]

5.3.1. Let \( F \) be a field, and \( n \) a positive integer. If \( z \) is an \( n \)-th root of 1, then \( z^{-1} \) is also an \( n \)-th root of 1. If \( x \) and \( y \) are two \( n \)-th roots of 1, then \( xy \) is an \( n \)-th root of 1.

Solution: We have \( z^n = 1 \), by the definition of \( n \)-th roots of 1. Hence the inverse of \( z \) is \( z^{n-1} \), and \( (z^{n-1})^n = (z^n)^{n-1} = 1 \) i.e. the inverse is also an \( n \)-th root of 1. We have \( x^n = 1 \) and \( y^n = 1 \). Multiplying this equations gives \( x^n y^n = 1 \). Since the multiplication in a field is commutative, \( x^n y^n = (xy)^n \), thus \( (xy)^n = 1 \), i.e. \( xy \) is an \( n \)-th root of 1.

5.3.3. Compute all powers of 2 modulo 13, and enter them in the table. Which numbers modulo 13 have order 12?

Solution.

| \(|I\) | \(01\) | \(02\) | \(03\) | \(04\) | \(05\) | \(06\) | \(07\) | \(08\) | \(09\) | \(10\) | \(11\) | \(12\) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| \(2^I\) | 2 | 4 | 8 | 3 | 6 | 12 | 11 | 9 | 5 | 10 | 7 | 1 |

The table shows that the order of 2 is 12. Since \( 2^I \) has order 12 if and only if \( I \) is prime to 12, it follows that \( 2, 2^5 = 6, 2^7 = 11, 2^{11} = 7 \) have order 12.

5.3.4. Calculate orders of all non-zero elements modulo 13.

Solution:

<table>
<thead>
<tr>
<th>(x)</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>(</td>
<td>\text{ord}(x)</td>
<td>)</td>
<td>1</td>
<td>12</td>
<td>3</td>
<td>6</td>
<td>4</td>
<td>12</td>
<td>12</td>
<td>4</td>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>

5.4.1. Use the discrete logarithm modulo 11 with base 2 to solve the congruence \( 7x \equiv 6 \pmod{11} \).

| \(|I\) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| \(2^I\) | 2 | 4 | 8 | 5 | 10 | 9 | 7 | 3 | 6 | 1 |
Solution: Using notation \( I(x) \) for the discrete logarithm, the equation \( 7x \equiv 6 \pmod{11} \) implies \( I(7) + I(x) \equiv I(6) \pmod{10} \). Using \( I(7) = 7 \) and \( I(6) = 9 \) from the above table, it follows that \( I(x) = 9 - 7 = 2 \). Hence \( x = 4 \).

6. Chapter 6

6.1.2 b) Use Euler’s criterion to determine if 2 is a square modulo 43. Compute the necessary power of 2 using the method of consecutive squares.

Solution: We need to compute \( 2^{(43-1)/2} = 2^{21} \) modulo 43. Consecutive squaring of 2 modulo 43 gives
\[
2^4 = 16, \quad 2^8 = 16^2 = -2, \quad 2^{16} = (-2)^2 = 4.
\]
Since \( 21 = 16 + 4 + 1 \), \( 2^{21} = 2^{16} \cdot 2^4 \cdot 2 \equiv 4 \cdot 16 \cdot 2 = 128 \equiv -1 \pmod{43} \). Hence 2 is not a square modulo 43.

6.4.1. Use the primitive root 2 modulo 37 to find a primitive cubic root modulo 37, and a square root of \(-3\) modulo 37.

Solution: 2 has order 36, hence \( 2^{12} \equiv -11 \pmod{37} \) and its square \( 2^{24} \equiv 10 \pmod{37} \) are of order 3, i.e. primitive cube roots of 1. Their difference \(-21 \equiv 16 \pmod{37} \) is a square root of \(-3\).

6.4.6 State the quadratic reciprocity law. Then calculate \( \left(\frac{122}{127}\right) \).

Solution: Note that \( 122 = 2 \cdot 61 \), \( 127 \equiv 7 \pmod{8} \) and \( 61 \equiv 5 \pmod{8} \). In particular 2 is a square modulo 127.
\[
\left(\frac{122}{127}\right) = \left(\frac{2}{127}\right) \cdot \left(\frac{61}{127}\right) = \left(\frac{61}{127}\right) = \left(\frac{127}{61}\right) = \left(\frac{5}{61}\right) = \left(\frac{61}{5}\right) = \left(\frac{1}{5}\right) = 1
\]

6.4.7. Does the quadratic equation \( x^2 + 4x + 11 = 0 \) have a solution modulo 43?

Solution: By completing to a square, roots of the quadratic equation are \(-2 \pm \sqrt{-7}\). By quadratic reciprocity,
\[
\left(\frac{-7}{43}\right) = \left(\frac{43}{7}\right) = \left(\frac{1}{7}\right) = 1.
\]
Hence, \(-7\) is a square modulo 43, so we have solutions modulo 43. Alternatively, notice that \(-7 \equiv 36 \pmod{43}\) so \(\sqrt{-7} = \pm 6\).

6.4.12. Let \( n \) be a positive integer. Let \( p \) be a prime divisor of \( n^2 + 3 \). Use the quadratic reciprocity to conclude that \( p \equiv 1 \pmod{3} \). Hint: \( n^2 \equiv -3 \pmod{p} \).

Solution: \( p \) dividing \( n^2 + 3 \) implies that \(-3\) is a square modulo \( p \). By the quadratic reciprocity, this happens if and only if \( p \equiv 1 \pmod{3} \).

6.4.13. Use the previous exercise to prove that there are infinitely many primes congruent to 1 modulo 3.
Solution: Let $S = \{p_1, \ldots, p_m\}$ be any set of primes congruent to 1 modulo 3. Let $n = p_1 \cdots p_m$. Then any $p$ dividing $n^2 + 3$ is clearly different from $p_1, \ldots, p_m$.

7. Chapter 7

7.1.5. Can Pepin’s test be done with 3 replaced by 7?

Solution: Yes if 7 is not a square modulo any Fermat’s prime. Thus we need to show that

$$\left(\frac{7}{F_n}\right) = -1,$$

for any Fermat prime $F_n$. Since $F_n \equiv 1 \pmod{4}$, it follows that

$$\left(\frac{7}{F_n}\right) = \left(\frac{F_n}{7}\right).$$

It remains to determine $F_n$ modulo 7. Note that consecutive squaring of 2 modulo 7 alternates between 2 and 4. Hence $F_n$, modulo 7, is 3 or 5. Neither of the two numbers is a square modulo 7, hence Pepin’s test works with 7.

8. Chapter 8

8.1.2. Use the descent procedure procedure to find a solution of the equation $x^2 + y^2 = 61$ starting with $11^2 + 1^2 = 2 \cdot 61$.

Solution: Here $m = 2$. $11 \equiv 1 \pmod{2}$ and $1 \equiv 1 \pmod{2}$.

$$\frac{1}{2}(11 + i)(1 - i) = 6 - 5i$$

giving $6^2 + 5^2 = 61$.

9. Chapter 9

9.1.4. Prove by induction the closed formula for the sum of the first $n$ powers of 2. (The first is $2^0 = 1$):

$$1 + 2 + \cdots + 2^{n-1} = 2^n - 1.$$ 

Solution: If $n = 1$ then $1 = 2^1 - 1$, so the formula is true for $n = 1$. Assume the formula true for $n$. Adding $2^n$ to both sides yields

$$1 + 2 + \cdots + 2^{n-1} + 2^n = 2^n - 1 + 2^n.$$ 

Since $2^n + 2^n = 2^n(1 + 1) = 2^n \cdot 2 = 2^{n+1}$, the formula is true for $n + 1$.

9.2.4. Show that, if $(u, v)$ is a solution of $x^2 - 3y^2 = -2$ then

$$\begin{cases} u_1 = 2u + 3v \\ v_1 = u + 2v \end{cases}$$

is another solution of $x^2 - 3y^2 = -2$. 
Solution:

\[(2u + 3v)^2 - 3(u + 2v)^2 = 4u^2 + 12uv + 9v^2 - 3(u^2 + 4uv + 4v^2) = u^2 - 3v^2 = -2.\]

NB: Solutions of the Pell equation \(x^2 - 3y^2 = 1\) “act” on the solutions of \(x^2 - 3y^2 = -2\). The first solution of \(x^2 - 3y^2 = 1\) is \(2 + \sqrt{3}\), and if \(u + v\sqrt{3}\) is a solution of \(x^2 - 3y^2 = -2\), then

\[(2 + \sqrt{3})(u + v\sqrt{3}) = (2u + 3v) + (u + 2v)\sqrt{3}\]

is another solution of \(x^2 - 3y^2 = -2\).

9.2.5. Recall that numbers \(P_n = \frac{3n^2 - n}{2}\) are pentagonal, while \(T_m = \frac{m(m+1)}{2}\) are triangular. The equation \(P_n = T_m\), after substituting \(n = (x + 1)/6\) and \(m = (y - 1)/2\), becomes the equation \(x^2 - 3y^2 = -2\). Use the previous problem to generate solutions of this equation to find three pentagonal-triangular numbers. \((P_1 = T_1 = 1\) is one.)

Solution: The first pentagonal-triangular number \(P_1 = T_1 = 1\) corresponds to the solution \((5, 3)\) of \(x^2 - 3y^3 = -2\). The previous exercise generates the following solutions of \(x^2 - 3y^2 = -2\):

\[(19, 11), (71, 41), (265, 153), (989, 571)\ldots\]

Only every other of these solutions can be converted into integral \((n, m)\): \((71, 41)\) into \((12, 20)\) and \((989, 571)\) into \((165, 285)\). It follows that

\[P_{12} = T_{20} = 210\] and \[P_{165} = T_{285} = 40755\]

are two additional pentagonal-triangular numbers.