Math 324, Fall 2010
Assignment 3
Solutions

Exercise 1. Find all the integral solutions of the following linear diophantine equations. Be sure to justify your answers.

(i) \(3x + 4y = 7\).
(ii) \(12x + 18y = 50\).
(iii) \(2x + 3y + 5z = 12\).

Solution:

(i) By inspection, \((x, y) = (1, 1)\) is a particular solution of the equation. Observing \(3, 4\) = 1, the general solution is

\[(x, y) = (1 + 4k, 1 - 3k), \quad k \in \mathbb{Z}.
\]

(ii) We note that \((12, 18) = 6\). Since 6 does not divide 50, the equation \(12x + 18y = 50\) has no integral solutions.

(iii) Let \((x, y, z)\) be an integral solution of the equation

\[2x + 3y + 5z = 12. \quad (1)
\]

Observing \((3, 5) = 1\), \((u, v) = (x, 3y + 5z)\) is a solution of the congruence

\[2x + v = 12.
\]

The last equation has the particular solution \((6, 0)\), hence the general solution

\[(x, v) = (6 + k, -2k), \quad k \in \mathbb{Z}.
\]

Observing

\[1 = 3 \cdot 2 + 5 \cdot (-1),
\]

multiplication by \(k\) shows that \((y, z) = (-4k, 2k)\) is a particular solution of the equation

\[-2k = 3y + 5z.
\]

Since \((3, 5) = 1\), the last equation has the general solution

\[(y, z) = (-4k + 5l, 2k - 3l), \quad l \in \mathbb{Z}.
\]

We conclude that the general solution of \((1)\) is

\[(x, y, z) = (6 + k, -4k + 5l, 2k - 3l), \quad k, l \in \mathbb{Z}.
\]

Exercise 2.

(i) Let \(m, n\) be positive integers with \(n|m\). Show that \(a \equiv b \mod m\) implies \(a \equiv b \mod n\). Deduce that the assignments

\[a \mod m \mapsto a \mod n
\]

give a ring homomorphism \(\mathbb{Z}/\mathbb{Z}m \to \mathbb{Z}/\mathbb{Z}n\).

(ii) Let \(a, b,\) and \(c\) be integers with \(c\) positive. If \(a \equiv b \mod c\), show \(\gcd(a, c) = \gcd(b, c)\).

Solution:

(i) If \(a \equiv b \mod m\) then \(m\) divides \(a - b\). Since \(n\) is assumed to divide \(m\), it follows that \(n\) divides \(a - b\), hence \(a \equiv b \mod m\).
In light of the preceding remarks, if \( a \mod m = a' \mod m \) then \( a \mod n = a' \mod n \). It follows that the rule
\[
a \mod m \mapsto a \mod n, \quad a \in \mathbb{Z},
\]
yields a well-defined map \( \rho : \mathbb{Z}/\mathbb{Z}m \to \mathbb{Z}/\mathbb{Z}n \). Furthermore, if \( a, b \in \mathbb{Z} \), we have
\[
\rho (a \mod m + b \mod m) = \rho ((a + b) \mod m) = (a + b) \mod n
= a \mod n + b \mod n = \rho (a \mod m) + \rho (b \mod m),
\]
and
\[
\rho (a \mod m \cdot b \mod m) = \rho (ab \mod m) = ab \mod n = a \mod n \cdot b \mod n = \rho (a \mod m) \cdot \rho (b \mod m).
\]
This shows that \( \rho \) respects both addition and multiplication, hence is a homomorphism as claimed.

(ii) The hypothesis \( a \equiv b \mod n \) implies there exists \( k \in \mathbb{Z} \) such that \( b = a + kn \). Exercise 1, Assignment 1 thus allows us to deduce
\[
(a, n) = (b - kn, n) = (n, b) = (b, n).
\]

Exercise 3. (i) Let \( n \) be a integer. Show that \((n + 3)^3 \equiv n^3 \mod 9\).
(ii) Let \( n \) be a natural number. Prove that
\[
n^3 + (n + 1)^3 + (n + 2)^3
\]
is divisible by 9. (Hint : You may find (i) useful.)

Solutions : (i) We calculate
\[
(n + 3)^3 = n^3 + 3n^2 \cdot 3 + 3n \cdot (3)^2 + 3^3 \equiv n^3 + 0 + 0 + 0 = n^3 \mod 9.
\]
(ii) We shall use induction on \( n \). Since
\[
0^3 + 1^3 + 2^3 = 0 + 1 + 8 = 9,
\]
the result is true for \( n = 3 \). Suppose
\[
n^3 + (n + 1)^3 + (n + 2)^3
\]
is divisible by 9. By part (i), there exists integer \( k \) such that
\[
(n + 3)^3 = n^3 + 9k.
\]
Therefore,
\[
(n + 1)^3 + (n + 2)^3 + (n + 3)^3 = (n + 1)^3 + (n + 2)^3 + n^3 + 9k.
\]
By hypothesis, the sum of the first three terms on the right is divisible by 9. Since the remaining term is clearly divisible by 9, the righthand side of (1) is divisible by 9. Thus,
\[
(n + 1)^3 + (n + 2)^3 + (n + 3)^3
\]
is divisible by 9. The Principle of Mathematical Induction allows us to conclude that the result holds for all natural numbers \( n \).

Exercise 4. Let \( m \) be a positive integer. If \( m \) is odd or divisible by 4, show that
\[
1^3 + 2^3 + 3^3 + \cdots + (m - 1)^3 \equiv 0 \mod m.
\]
Is the statement true if \( m \) is even but not divisible by 4 ?
Solution: Set
\[ S_{m-1} = 1^3 + 2^3 + 3^3 + \cdots + (m-1)^3. \]

Using induction on \( m \), it is readily proved that
\[ S_{m-1} = \frac{m^2(m-1)^2}{4}. \]

If \( m \) is odd then \( m-1 \) is even. Writing \( m-1 = 2l \), we obtain
\[ S_{m-1} = \frac{m^2(2l)^2}{4} = m^2l^2. \]

This shows \( m \) divides \( S_{m-1} \), hence \( S_{m-1} \equiv 0 \mod m \).

If \( m \) is divisible by 4, say \( m = 4k \), then
\[ S_{m-1} = \frac{m^2(m-1)^2}{4} = \frac{m(4k)(m-1)^2}{4} = mk(m-1)^2. \]

Thus \( m \) divides \( S_{m-1} \), hence \( S_{m-1} \equiv 0 \mod m \).

If \( m \) is even but not divisible by 4 then the Division Algorithm yields \( m = 4k + 2 \) for some integer \( k \). In this case,
\[ S_{m-1} = \frac{m^2(m-1)^2}{4} = \frac{(4k+2)(m-1)^2}{4} = (2k+1)^2(m-1)^2. \]

In particular, \( S_{m-1} \) is odd. Since any multiple of \( m \) will be even, we conclude \( m \) does not divide \( S_{m-1} \), hence \( S_{m-1} \not\equiv 0 \mod m \). In fact, one has
\[ S_{m-1} = (2k+1)^2(m-1)^2 \equiv (2k+1)^2(-1)^2 = (2k+1)^2 = \frac{m^2}{4} \mod m. \]

Alternate Solution: If \( 1 \leq j \leq m-1 \) then
\[ -j \equiv m-j \mod m, \]

hence
\[ -j^3 = (-j)^3 \equiv (m-j)^3 \mod m. \] (1)

If \( m \) is odd then \( m-1 \) is even. Writing \( m-1 = 2l \), we have
\[ S_{m-1} = \sum_{j=1}^{l} j^3 + \sum_{j=l+1}^{2l} j^3. \]

Changing the index from \( j \) to \( 2l+1-j \) and reversing the order of summation, the second sum appearing on the right can be rewritten as
\[ \sum_{j=1}^{2l} j^3 = \sum_{j=1}^{l} (2l+1-j)^3 = \sum_{j=1}^{l} (m-j)^3. \]

Substituting in our expression for \( S_{m-1} \) and using (1), we obtain
\[ S_{m-1} = \sum_{j=1}^{l} j^3 + \sum_{j=1}^{l} (m-j)^3 = \sum_{j=1}^{l} (j^3 + (m-j)^3) \equiv \sum_{j=1}^{l} (j^3 - j^3) = \sum_{j=1}^{l} 0 = 0 \mod m. \]
Suppose $m$ is even, say $m = 2k$. In this case, the sum $S_{m-1}$ consists of $2k - 1$ terms. The argument provided above shows that the first $k - 1$ terms are cancelled modulo $m$ by the last $k - 1$ terms. As such,

$$S_{m-1} \equiv k^3 = \left(\frac{m}{2}\right)^3 \mod m.$$ 

If $m$ is divisible by 4, say $m = 4l$ then

$$S_{m-1} \equiv \left(\frac{m}{2}\right)^3 = (2l)^3 = 8l^3 = 4l \cdot 2l^2 = m \cdot 2l^2 \equiv 0 \mod m.$$

On the other hand, if $m$ is not divisible by 4, say $m = 4n + 2$, then

$$S_{m-1} \equiv \left(\frac{m}{2}\right)^3 = (2n + 1)^3 \mod m.$$ 

Observing $m$ cannot divide $(2n + 1)^3$, since the latter number is odd, we conclude $S_{m-1} \not\equiv 0 \mod m$ if $m$ is even but not divisible by 4.

**Exercise 5.** Let $p$ be prime. Show that the only solutions of the congruence

$$x^2 \equiv x \mod p$$ 

correspond to the integers $x$ such that $x \equiv 0$ or $1 \mod p$.

**Solution:** If $x$ is a solution of the given congruence then $p$ divides

$$x^2 - x = x(x - 1).$$

Since $p$ is prime, we conclude that either $p | x$ or $p | (x - 1)$, hence $x \equiv 0 \mod p$ or $x \equiv 1 \mod p$.

**Exercise 6.** (a) Solve the following linear congruences

(i) $128x \equiv 833 \mod 1001$.
(ii) $987x \equiv 610 \mod 1597$.

(b) For which integers $c$, $0 \leq c < 30$, does the congruence

$$12x = c \mod 30$$

have solutions? When there are solutions, how many incongruent solutions are there?

**Solutions:** (a) (i) Using the Euclidean Algorithm, we calculate $\gcd(128, 1001) = 1$, with

$$1 = 305 \cdot 128 - 39 \cdot 1001.$$ 

The preceding allows us to conclude that 305 is an inverse modulo 1001 of 128, hence the equation has the unique solution

$$x \equiv 305 \cdot 833 \equiv 305 \cdot (-168) = -51240 \equiv -189 \mod 1001.$$ 

(ii) By inspection,

$$x \equiv -1 \mod 1597$$

is a solution of the congruence. Indeed,

$$-987 \equiv 1597 - 987 = 610 \mod 1597.$$ 

Using the Euclidean Algorithm, we calculate $\gcd(987, 1597) = 1$, hence $x \equiv -1 \mod 1597$ is the unique solution modulo 1597.
(b) We note that \( d = \gcd(12, 30) = 6 \). From the result in class, the congruence

\[ 12x \equiv c \mod 30 \]

has a solution if and only if \( c \) is divisible by 6, i.e.

\[ c \in \{0, 6, 12, 18, 24\}. \]

In each case, the congruence has \( d = 6 \) incongruent solutions modulo 30.

**Exercise 7.** (a) Let \( p \) be an odd prime and \( a \in \mathbb{Z} \). Show that the equation

\[ x^2 \equiv a \mod p \]

either has no solution or exactly two incongruent solutions.

(b) Consider the congruence

\[ x^2 \equiv 1 \mod 2^k \]

(i) Show that (1) has one solution when \( k = 1 \).

(ii) Show that (1) has two incongruent solutions when \( k = 2 \).

(iii) Show that (1) has four incongruent solutions when \( k > 2 \), namely \( x = \pm 1 \) or \( \pm (1 + 2^{k-1}) \).

**Solutions**

(a) Suppose the congruence has a solution, say \( x_0 \). If \( x \) is a second solution, then

\[ x^2 \equiv a \equiv x_0^2 \mod p, \]

hence

\[ 0 \equiv x^2 - x_0^2 \mod p. \]

In particular, \( p \) divides

\[ x^2 - x_0^2 = (x - x_0)(x + x_0). \]

Since it is prime, \( p \) must either divide \( x - x_0 \) or \( x + x_0 \), hence \( x \equiv \pm x_0 \mod p \). This shows that the congruence has at most two incongruent solutions. If

\[ x_0 \equiv -x_0 \mod p \]

then \( p \) divides \( x_0 - (-x_0) = 2x_0 \). Since \( p \) is an odd, \( p \) does not divide 2, hence \( p \mid x_0 \), \( p \) being prime. In this case, \( x_0 \equiv 0 \mod p \), hence

\[ a \equiv x_0^2 \equiv 0^2 = 0 \mod p, \]

which implies \( p \) divides \( a \), a contradiction. Thus \( x_0 \) and \( -x_0 \) provide two incongruent solutions modulo \( p \).

In light of the above, the congruence

\[ x^2 \equiv a \mod p \]

either has no solution or exactly two incongruent solutions.

(b)(i) By the Division Algorithm, every integer is congruent to 0 or 1 modulo 2. Observing

\[ 0^2 = 0 \not\equiv 1 \mod 2 \]

while

\[ 1^2 = 1 \equiv 1 \mod 2, \]

the congruence

\[ x^2 \equiv 1 \mod 2 \]

has the unique solution \( x \equiv 1 \mod 2 \).
(ii) If $x$ is even then $x^2 - 1$ is odd; in particular it is not divisible by 4. It follows that if $x$ is a solution of the congruence

$$x^2 \equiv 1 \mod 4$$

then $x$ is odd. In this case, the Division Algorithm ensures that $x$ is congruent to either 1 or 3. Since

$$1^2 = 1$$

and

$$3^2 = 9 \equiv 1 \mod 4,$$

we see that the solution set consists of the congruence classes of 1 and 3. Since $1 \not\equiv 3 \mod 4$, we deduce that the congruence

$$x^2 \equiv 1 \mod 4$$

has precisely two incongruent solutions.

(iii) Let $r$ be an arbitrary solution of the congruence

$$x^2 \equiv 1 \mod 2^k. \quad (1)$$

First note that $r$ is necessarily odd. As such, both $r + 1$ and $r - 1$ are even, so Exercise 4, Assignment 1 allows us to conclude

$$\gcd(r - 1, r + 1) = 2.$$

We now consider cases.

(I) The exponent of 2 in the prime factorization of $r - 1$ is 1. In this case, we can write

$$r - 1 = 2l$$

where $l$ is odd. The congruence (1) thus yields

$$0 \equiv r^2 - 1 = (r - 1)(r + 1) = 2l(r + 1) \mod 2^k.$$

Cancelling the factor of 2,

$$0 \equiv l(r + 1) \mod 2^{k-1}.$$

Being odd, $l$ is invertible modulo $2^{k-1}$. Multiplying by an inverse, we see

$$0 \equiv (r + 1) \mod 2^{k-1},$$

hence

$$r = -1 + q2^{k-1}$$

for some integer $q$. If $q$ is odd then $r \equiv -1 + 2^{k-1} \mod 2^k$, while $r \equiv -1 \mod 2^k$ if $q$ is even.

(II) The exponent of 2 in the prime factorization of $r + 1$ is 1. In this case, we can write

$$r + 1 = 2l$$

where $l$ is odd. The congruence (1) thus yields

$$0 \equiv r^2 - 1 = (r - 1)(r + 1) = 2l(r - 1) \mod 2^k.$$

Cancelling the factor of 2,

$$0 \equiv l(r - 1) \mod 2^{k-1}.$$

Being odd, $l$ is invertible modulo $2^{k-1}$. Multiplying by an inverse, we see

$$0 \equiv (r - 1) \mod 2^{k-1},$$
hence

\[ r = 1 + q2^{k-1} \]

for some integer \( q \). If \( q \) is odd then \( r \equiv 1 + 2^{k-1} \mod 2^k \), while \( r \equiv 1 \mod 2^k \) if \( q \) is even.

If \( x, y \in \{-1, 1, -1 + 2^{k-1}, 1 + 2^{k-1}\} \) then, since \( k > 2 \),

\[ |x - y| < 2 + 2^{k-1} < 2^{k-1} + 2^{k-1} = 2^k. \]

Thus, \( x - y \) is divisible by \( 2^k \) if and only if \( x - y = 0 \), i.e. \( x = y \). In particular, the elements of \( \{-1, 1, -1 + 2^{k-1}, 1 + 2^{k-1}\} \) yield distinct congruence classes modulo \( 2^k \), hence distinct solutions modulo \( 2^k \) of the congruence (1).

The preceding discussion allows to deduce that the congruence has precisely four incongruent solutions when \( k \geq 3 \).