Homework 5 Solutions

Tim Smits

1. Compute the following:

(a) $9284756 \bmod 8$

(b) $-181374 \bmod 29$

(c) $-3287943 \bmod 823$

Solution: Details are omitted.

(a) $4 \bmod 8$

(b) $21 \bmod 29$

(c) $765 \bmod 823$

2. Reduce the following:

(a) $1294 \cdot 293452 + 96273 \cdot 4751 \bmod 9$

(b) $84526 \cdot 862967^3 - 448184 \cdot 591183^2 \bmod 15$

(c) $(-823529) \cdot 19581 - 234603^3 \bmod 23$

Solution: Details are omitted.

(a) $4 \bmod 9$

(b) $2 \bmod 15$

(c) $22 \bmod 23$

3.Compute the following:

(a) $3^{-1} \bmod 8$

(b) $16^{-1} \bmod 29$

(c) $14^{-1} \bmod 4914$

Solution: Use the Euclidean algorithm to find a pair of integers x, y such that $ax + ny = 1$, where you want to find the inverse of $a \bmod n$, so that $a^{-1} \bmod n \equiv x \bmod n$. The details are omitted.

(a) $3 \bmod 8$

(b) $20 \bmod 29$

(c) No solution, since $\gcd(14, 4914) \neq 1$.

4. Solve the following:

(a) $3x \equiv 7 \bmod 8$

(b) $1723x \equiv 3574 \bmod 4914$

(c) $-3245x \equiv 5722 \bmod 71$

Solution: Find the inverse of a mod n and multiply through to solve for x mod n. Details are omitted.

(a) $x \equiv 5 \bmod 8$

(b) $x \equiv 2104 \bmod 4914$

(c) $x \equiv 2 \bmod 71$

5. Reduce the following, and then find k such that $a^k \equiv 1 \bmod n$

(a) $1769^{234} \bmod 31$

(b) $6247^{5138} \bmod 14$

(c) $289^{63251} \bmod 432$

Solution: Details are omitted.

(a) 16 mod 31 and $k = 5$.

(b) 9 mod 14 and $k = 6$.

(c) 145 mod 432 and $k = 3$.

6. Check whether or not a^{-1} exists by computing (a, n). Then use this to prove there is no solution to each congruence equation.

(a) $10x \equiv 31 \bmod 42$

(b) $18x \equiv 20 \bmod 60$

(c) $63x \equiv 35 \bmod 105$

Solution:

(a) We note that $\gcd(10, 42) = 2$. If $10x \equiv 31 \bmod 42$, then there are integers x, y such that $10x + 42y = 31$. However, $2 \nmid 31$, so this is a contradiction.

(b) We note that $\gcd(18, 60) = 6$. If $18x \equiv 20 \bmod 60$, then there are integers x, y such that $18x + 60y = 20$, which is a contradiction because $6 \nmid 20$.

(c) We note that $\gcd(63, 105) = 21$. If $63x \equiv 35 \bmod 105$ is solvable, there are integers x, y such that $63x + 105y = 35$, which is impossible since $21 \nmid 35$.

7. Check whether or not a^{-1} exists by computing (a, n), and solve the congruence equation.

(a) $10x \equiv 34 \bmod 42$

(b) $18x \equiv 36 \bmod 60$

(c) $63x \equiv 21 \bmod 105$

Solution: Find the inverse of a mod n and multiply through to solve for x mod n. Details are omitted.

(a) $x \equiv 16 \bmod 42$

(b) $x \equiv 2 \bmod 60$

(c) $x \equiv 2 \bmod 105$

8. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$, and let $g = \gcd(a, n)$. Prove that there exists $x \in \mathbb{Z}$ such that $ax \equiv b \bmod n$ if and only if $g \mid b$, and that in this case, the solution is given by $x \equiv a'^{-1}b' \bmod (n')$, where $a = ga'$, $b = gb'$, and $n = gn'$ for some integers a', b', n'.

Solution: If $ax \equiv b \bmod n$, is solvable, then there are integers x, y such that $ax + ny = b$. Since $g \mid a$ and $g \mid n$, this says $g \mid b$. Conversely, suppose that $g \mid b$. Write $a = ga'$, $b = gb'$, and $n = gn'$ for some integers a', b', n'. Since $\gcd(a', n') = 1$, by Bezout there are integers x, y such that $a'x + n'y = 1$, so multiplying by b' says $a'(xb') + n'(yb') = b'$. Multiplying through by g then says $a(xb') + n(yb') = b$, so that $a(xb') \equiv b \bmod n$, so that the congruence is solvable.

When $ax \equiv b \bmod n$ has a solution, then $ax + ny = b$ for some integers x, y. Then dividing through by g says that $a'x + n'y = b'$, so $a'x \equiv b' \bmod n'$. Since a' is invertible mod n', the solution is given by $x \equiv a'^{-1}b' \bmod n'$.