Homework 2, Solutions

\(1.33\)(a) Find a single value \(x\) that simultaneously solves the two congruences.

\[ x \equiv 3 \pmod{7} \quad \text{and} \quad x \equiv 4 \pmod{9} \]

**Solution:** Since \(x \equiv 3 \pmod{7}\), as an integer, \(x = 3 + 7y\) for some integer \(y\). Substitute \(x = 3 + 7y\) into \(x \equiv 4 \pmod{9}\) to get \(3 + 7y \equiv 4 \pmod{9}\).

Now we solve \(3 + 7y \equiv 4 \pmod{9}\) by adding \(-3 \pmod{9}\) both sides. This yields \(7y \equiv 1 \pmod{9}\).

To find \(7^{-1} \pmod{9}\), we use Euclidean Algorithm (you can also use matlab) to get \(1 = \gcd(7, 9) = (4)(7) + (-3)(9)\), and so \(7^{-1} \equiv 4 \pmod{9}\). Hence \(y \equiv (4)(7y) \equiv 4 \pmod{9}\), or \(y = 4 + 9m\) for an integer \(m\). Therefore, the smallest positive solution of \(x\) is \(x = 31\).

\(1.28\)(a) Here in this exercise, \(ord_2(2816)\) asks the exponent of 2 in the unique factorization of 2816.

**Solution:** We can factor \(2816 = 4(704) = (4)(4)(176) = (4)(4)(16)(11) = 2^8(11)\), and so \(ord_2(2816) = 8\).

\(1.32\)(a) For each of the following primes is 2 a primitive root modulo \(p\)?

**Solutions:**

(i) \(p = 7\). We compute that \(2^2 \equiv 4, 2^3 \equiv 1 \pmod{7}\). Therefore, the order of 2 (mod 7) is 3, \((\not 6)\), and so 2 is not a primitive root mod 7.

(ii) \(p = 13\). We compute that \(2^2 \equiv 4, 2^4 \equiv 8, 2^4 \equiv 3, 2^5 \equiv 6, \ldots, 2^{12} \equiv 1 \pmod{13}\). Therefore, the order of 2 (mod 13) is 12, and so 2 is a primitive root mod 13.

(iii) \(p = 19\). We compute that \(2^2 \equiv 4, 2^4 \equiv 8, 2^4 \equiv 16 \equiv -3, 2^5 \equiv -6 \equiv 13, 2^6 \equiv -12 \equiv 7, 2^7 \equiv 14 \equiv -2, 2^8 \equiv -4 \equiv 15, 2^9 \equiv -8 \equiv 11, \ldots, 2^{18} \equiv 1 \pmod{19}\). Therefore, the order of 2 (mod 19) is 18, and so 2 is a primitive root mod 19.

(iv) \(p = 23\). We compute that \(2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 16 \equiv -6, 2^5 \equiv -12 \equiv 11, 2^6 \equiv 22 \equiv -1, 2^{12} \equiv 2^6 \cdot 2^6 \equiv 1 \pmod{23}\). Therefore, the order of 2 (mod 23) is 12, \((\not 22)\), and so 2 is not a primitive root mod 23.

\(1.34\)(a) Let \(p\) be an odd prime and let \(b\) be an integer with \(p \nmid b\). Prove that either \(b\) has two square roots modulo \(p\) or else \(b\) has no square roots modulo \(p\).
Proof: It suffices to show that if $b$ has at least one square root modulo $p$, then $b$ must have exactly two square roots modulo $p$.

Suppose that $a$ is a square root of $b$ mod $p$. Since $p \nmid b$, $a \not\equiv 0 \pmod p$. Therefore, $p \nmid a$ and so $gcd(a, p) = 1$.

Since $a^2 \equiv b \pmod p$, it follows that $(-a)^2 \equiv a^2 \equiv b \pmod p$, and so $-a$ must also be a square root of $b$ (mod $p$). We need to explain that $a \equiv -a \pmod p$. If we had $a \equiv -a \pmod p$, then $2a \equiv 0 \pmod p$, and so $p\lvert (2a)$. Since $gcd(a, p) = 1$, that $p\lvert (2a)$ and $gcd(a, p) = 1$ imply that $p\lvert 2$, contrary to the assumption that $p$ is an odd prime. Hence $a \not\equiv -a \pmod p$, and so $b$ has at least two square roots.

We need to show that $b$ cannot have more than 2 square roots. Suppose that for some $c \in \mathbb{Z}_p$ such that $c \not\equiv a \pmod p$ and $c \not\equiv -a \pmod p$ but $c^2 \equiv b \pmod p$. Then we have $a^2 \equiv b \equiv c^2 \pmod p$, or equivalently, $(a - c)(a + c) \equiv a^2 - c^2 \equiv b - b \equiv 0 \pmod p$. This means in integers, $p\lvert (a - c)(a + c)$. Since $p$ is a prime, either $p\lvert (a - c)$, whence $c \equiv a \pmod p$; or $p\lvert (a + c)$, whence $c \equiv -a \pmod p$. Either way will lead to a contradiction to the assumption that $c \not\equiv a \pmod p$ and $c \not\equiv -a \pmod p$. Thus, $b$ must have exactly two square roots, if it has at least one.

(1.34)(b)(i) Find solution(s) of $x^2 \equiv b \pmod p$, with $(p, b) = (7, 2)$. This is to find solution(s) of $x^2 \equiv 2 \pmod 7$.

Solutions: We compute that $2^2 \equiv 4$, $3^2 \equiv 2$, $4^2 \equiv (-3)^2 \equiv 2$, $5^2 \equiv (-2)^2 \equiv 4 \pmod 7$. Therefore, $x^2 \equiv 2 \pmod 7$ has solutions $x \equiv 3, 4$ in $\mathbb{Z}_7$. 

2