COMP 2711H Discrete Mathematical Tools for Computer Science
Solutions to Tutorial 4

QB2-2. Use Euclid's extended GCD algorithm to find the multiplicative inverse in Z_{1009} for (a)17, (b)100, and (c) 777.

Solution

(a) We run Euclidean algorithm on $(1009, 17)$. We have that

$$\begin{aligned} 1009 &= 59 * 17 + 6 \\ 17 &= 2 * 6 + 5 \\ 6 &= 1 * 5 + 1. \end{aligned}$$

Then we work backwards to find the inverse of 17 modulo 1009.

$$\begin{aligned} 1 &= 6 - 5 & &= 6 - (17 - 2 * 6) \\ &= -17 + 3 * 6 & &= -17 + 3 * (1009 - 59 * 17) \\ &= 3 * 1009 - 178 * 17 \end{aligned}$$

So, the inverse of 17 modulo 1009 is $(1009 - 178) = 831$.

(b) 111

(c) 735

Hint When a is divided by b, and the quotient is c and the remainder is r, we have $a = b \cdot c + r$. And we suppose $d = gcd(a, b) = gcd(b, r)$.

If we have a linear expression of b and r, $d = b \cdot x + r \cdot y$, then we can rewrite r as $a - b \cdot c$, so we get a linear expression of a and b,

$$d = b \cdot x + (a - b \cdot c) \cdot y = a \cdot y + b \cdot (x - c \cdot y)$$

QB2-3. Show that if m is not prime, then at least $\sqrt{m}$ elements of Z_m do not have multiplicative inverses. Problem 5

Solution For any $a \in Z_m$, we know that a has inverse modulo m if and only if a and m are co-prime. Hence, to prove that at least $\sqrt{m}$ elements of Z_m do not have multiplicative inverses, it suffices to show that at least $\sqrt{m}$ elements of Z_m are not relatively prime to m. Since m is not prime, there is some integer $a \in Z_m$ such that $a|m$ and $a > 1$. Without loss of generality, we assume $a \leq \sqrt{m}$ since otherwise we can take the number m/a. Now consider $S = \{0, a, 2a, \ldots, (\lceil\sqrt{m}\rceil - 1)a\} \subseteq Z_m$. One can easily see that all these $\lceil\sqrt{m}\rceil$ numbers in S are not relatively prime to m.

QB2-4. Prove that if $x^{n-1} \equiv 1$ (modulo n) for all integers x that are not multiples of n, then n is prime.

Solution Recall that an integer a is relatively prime to n if and only if a has a inverse modulo n. To prove that n is a prime, it suffices to show that for any number $a \in \{1, \ldots, n-1\}$, a is relatively prime to n, or equivalently, a has a inverse modulo n. Note that for any $a \in \{1, \ldots, n-1\}$, a is not a multiple of n. By the hypothesis, we have that

$$a^{n-1} \equiv 1 \pmod{n}.$$

Hence, $(a^{n-2} \bmod n)$ is the inverse of a modulo n. This completes the proof.

EP2-13. Show that for any integer n, exactly one of $n, n+2, n+4$ is divisible by 3. In particular, except for 3,5,7, there are no triples of prime numbers occurring in the pattern $n, n+2, n+4$.

Solution There is exactly one number divisible by 3 among every three consecutive numbers $a, a+1, a+2$.

- If $a \equiv 0 \mod 3$, then a is the number divisible by 3 and $a+1, a+2$ are not.
- If $a \equiv 1 \mod 3$, then $a+2$ is the number divisible by 3 and $a, a+1$ are not.
- If $a \equiv 2 \mod 3$, then $a+1$ is the number divisible by 3 and $a, a+2$ are not.

If

$$n \equiv a \mod 3$$

then,

$$n+2 \equiv a+2 \mod 3$$

$$n+4 \equiv a+1 \mod 3$$

So exactly one of $n, n+2, n+4$ is divisible by 3.

Because one of $n, n+2, n+4$ is divisible by 3. If $n > 3$, there will be a number equals to $3 \cdot t$, which is not a prime, so $n \leq 3$. The only triple is $(3, 5, 7)$.

EP2-17. Compute the value of $7^{3(2k+1)} \mod 43$, where $k \in \mathbb{Z}^+$.

Solution

$$7^2 = 49 \equiv 6 \mod 43$$

$$7^3 \equiv 6 \cdot 7 = 42 \equiv -1 \mod 43$$

So that,

$$7^{3(2k+1)} \equiv (-1)^{2k+1} \equiv -1 \mod 43$$