CSE 311: Foundations of Computing I

Section 5: Number Theory Solutions

1. Casting Out Nines

Let $n \in \mathbb{N}$. Prove that if $n \equiv 0 \pmod 9$, then the sum of the digits of n is a multiple of 9.
You may use without proof that $a \equiv b \pmod m \rightarrow a^i \equiv b^i \pmod m$.

Solution:

Suppose $n \equiv 0 \pmod 9$, where $n = (x_m x_{m-1} \cdots x_1 x_0)_{10}$ (This is because we are working with a base-10 number). Then, it follows that $\sum_{i=0}^{m} x_i 10^i \equiv 0 \pmod 9$. Note that $10 \bmod 9 = 1$. Simplifying, we have:

$$
\begin{aligned}
n \equiv 0 \pmod 9 &\leftrightarrow \sum_{i=0}^{m} x_i 10^i \equiv 0 \pmod 9 && \text{[Definition of } n\text{]} \\
&\leftrightarrow \sum_{i=0}^{m} (x_i 10^i \bmod 9) \equiv 0 \pmod 9 && \text{[Additivity of Congruences]} \\
&\leftrightarrow \sum_{i=0}^{m} (x_i \bmod 9)(10^i \bmod 9) \equiv 0 \pmod 9 && \text{[Multiplicity of Congruences]} \\
&\leftrightarrow \sum_{i=0}^{m} (x_i \bmod 9)((10 \bmod 9)^i) \equiv 0 \pmod 9 && \text{[***]} \\
&\leftrightarrow \sum_{i=0}^{m} (x_i \bmod 9)((1 \bmod 9)^i) \equiv 0 \pmod 9 && \text{[Definition of mod]} \\
&\leftrightarrow \sum_{i=0}^{m} (x_i \bmod 9)(1) \equiv 0 \pmod 9 && \text{[Simplifying]} \\
&\leftrightarrow \sum_{i=0}^{m} x_i \equiv 0 \pmod 9 && \forall a, a \bmod 9 \equiv a \pmod 9
\end{aligned}
$$

This is what we were trying to prove.

*****:** This step is justified by the the property $a \equiv b \pmod m \rightarrow a^i \equiv b^i \pmod m$ for $a = 10$ and $b = 10 \bmod 9$. Since $10 \equiv 10 \bmod 9 (\bmod 9)$, $10^i \equiv (10 \bmod 9)^i (\bmod 9)$.

2. GCD

(a) Calculate gcd(100, 50).

(b) Calculate gcd(17, 31).

(c) Find the multiplicative inverse of 6 modulo 7.

(d) Does 49 have an multiplicative inverse modulo 7?

(e) Find the multiplicative inverse of 7 modulo 311.

(f) Find the multiplicative inverse of 27 modulo 151.

Solution:

a) 50

b) 1

c) 6

d) It does not. Intuitively, this is because 49x for any x is going to be 0 mod 7, which means it can never be 1.

e) 89

f) 28

3. Extended Euclidean Algorithm

(a) Find the multiplicative inverse y of 7 mod 33. That is, find y such that $7y \equiv 1 \pmod{33}$. You should use the extended Euclidean Algorithm. Your answer should be in the range $0 \leq y < 33$.

(b) Now, solve $7z \equiv 2 (\text{mod } 33)$.

Solution:

Part (a) First, we find the gcd:

$$\begin{aligned} \gcd(33,7) &= \gcd(7,5) & 33 &= \boxed{7} \bullet 4 + 5 && (1)\\ &= \gcd(5,2) & 7 &= \boxed{5} \bullet 1 + 2 && (2)\\ &= \gcd(2,1) & 5 &= \boxed{2} \bullet 2 + 1 && (3)\\ &= \gcd(1,0) & 2 &= 1 \bullet 2 + 0 && (4)\\ &= 1 && && (5) \end{aligned}$$

Next, we re-arrange equations (1) - (3) by solving for the remainder:

$$\begin{aligned} 1 &= 5 - \boxed{2} \bullet 2 && (6)\\ 2 &= 7 - \boxed{5} \bullet 1 && (7)\\ 5 &= 33 - \boxed{7} \bullet 4 && (8)\\ & && (9) \end{aligned}$$

Now, we backward substitute into the boxed numbers using the equations:

$$\begin{aligned} 1 &= 5 - \boxed{2} \bullet 2\\ &= 5 - (7 - \boxed{5} \bullet 1) \bullet 2\\ &= 3 \bullet \boxed{5} - 7 \bullet 2\\ &= 3 \bullet (33 - \boxed{7} \bullet 4) - 7 \bullet 2\\ &= 33 \bullet 3 + 7 \bullet -14 \end{aligned}$$

So, $1 = 33 \bullet 3 + \boxed{7} \bullet -14$. Thus, $33 - 14 = 19$ is the multiplicative inverse of 7 mod 33.

Part (b) If $7y \equiv 1 (\text{mod } 33)$, then

$$2 \cdot 7y \equiv 2 (\text{mod } 33).$$

So, $z \equiv 2 \times 19 (\text{mod } 33) \equiv 5 (\text{mod } 33)$.

4. Modular Exponentiation

Compute $7^{18} \bmod 23$ using the efficient modular exponentation algorithm. Show your intermediate results.

Solution:

First we calculate

- $7^1 \equiv 7(\text{ mod } 23)$.
- $7^2 = 49 \equiv 3(\text{ mod } 23)$.
- $7^4 \equiv 3^2(\text{ mod } 23) \equiv 9(\text{ mod } 23)$.
- $7^8 \equiv 9^2(\text{ mod } 23) \equiv 12(\text{ mod } 23)$.
- $7^{16} \equiv 12^2(\text{ mod } 23) \equiv 6(\text{ mod } 23)$.

Therefore,

$$7^{18} \equiv 7^{16} \times 7^2(\text{ mod } 23) \equiv 6 \times 3(\text{ mod } 23) \equiv 18(\text{ mod } 23).$$

5. More Number Theory

(a) Prove that if $n^2 + 1$ is a perfect square, where n is an integer, then n is even.

Solution:

We give two proofs:

Proof 1. Suppose $n^2 + 1$ is a perfect square. Then, by definition of perfect square, $n^2 + 1 = k^2$ for some $k \in \mathbb{Z}$. Suppose for contradiction that n is odd. Then,

$$n^2 + 1 = (2j + 1)2 + 1 = 4j^2 + 4j + 1 + 1 = 4(j^2 + j) + 2.$$

So, $n^2 + 1$ is even and $n^2 + 1 \bmod 4 = 2$, i.e., $4 \not| n^2 + 1$. Now, if k is odd, then $n^2 + 1 = k^2$ is odd which is a contradiction. And, if k is even $n^2 + 1 = k^2$ is divisible by 4 which is also a contradiction. Therefore, n is even.

Proof 2. Suppose $n^2 + 1$ is a perfect square. Then, by definition of perfect square, $n^2 + 1 = k^2$ for some $k \in \mathbb{N}$. Since n and k are integers, we can define some integer z such that $k = n + z$. Now, substituting, we get:

$$\begin{aligned} n^2 + 1 &= (n + z)^2 \\ n^2 + 1 &= n^2 + 2nz + z^2 \\ 1 &= 2nz + z^2 \\ 1 &= z(2n + z) \\ \frac{1}{z} &= (2n + z) \end{aligned}$$

Since n and z are integers, $2n + z$ is an integer, which means $\frac{1}{z}$ is an integer. The only integers which satisfy this constraint are $z = \pm 1$, and in both these cases $z = \frac{1}{z}$, so we can subtract z from both sides to find $n = 0$ as the only solution. Since $n = 0$, and 0 is even, n is even.

(b) Prove that if n is a positive integer such that the sum of the divisors of n is $n + 1$, then n is prime.

Solution:

Note that $n \mid n$. If the sum of divisors of n is $n + 1$, then $n + 1 - n = 1$ must be the only other divisor. It follows, by definition of prime, that n is prime.