CSE 311: Foundations of Computing I

Section 5: Number Theory Solutions

1. Modular Arithmetic

(a) Prove that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

Solution:

Suppose $a \mid b$ and $b \mid a$, where a, b are integers. By the definition of divides, we have $a \neq 0$, $b \neq 0$ and $b = ka, a = jb$ for some integers k, j. Combining these equations, we see that $a = j(ka)$.

Then, dividing both sides by a, we get $1 = jk$. So, $\frac{1}{j} = k$. Note that j and k are integers, which is only possible if $j, k \in \{1, -1\}$. It follows that $b = -a$ or $b = a$.

(b) Prove that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv b \pmod{m}$, where a and b are integers, then $a \equiv b \pmod{n}$.

Solution:

Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$. By definition of divides, we have $m = kn$ for some $k \in \mathbb{Z}$. By definition of congruence, we have $m \mid a - b$, which means that $a - b = mj$ for some $j \in \mathbb{Z}$. Combining the two equations, we see that $a - b = (knj) = n(kj)$. By definition of congruence, we have $a \equiv b \pmod{n}$, as required.

2. 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:

As we saw in lecture, if $a \equiv b \pmod{m}$, then $a + c \equiv b + c \pmod{m}$ and $ac \equiv bc \pmod{m}$. More generally, we can replace a with b in any expression involving only addition (or subtraction) and multiplication, and the result will still be congruent modulo m. We will use that fact to complete this proof.

Suppose that $n \equiv 0 \pmod 9$. Write n in terms of its decimal digits as $n = x_0 + 10x_1 + 10^2x_2 + \cdots + 10^mx_m$. The latter is an expression using only addition and multiplication, so we can replace all occurrences of 10 with any value congruent to it and the result will be congruent to n. Since $10 = 1 \cdot 9 + 1$, we see that $10 \equiv 1 \pmod 9$, so we can substitute 1 for 10 if we work mod 9.

Carrying out that calculation gives us:

$0 \equiv n \pmod 9$	Given
$\equiv x_0 + 10x_1 + 10^2x_2 + \cdots + 10^mx_m \pmod 9$	Definition of x_i's.
$\equiv x_0 + 1x_1 + 1^2x_2 + \cdots + 1^mx_m \pmod 9$	Substitute 1 for 10.
$\equiv x_0 + x_1 + x_2 + \cdots + x_m \pmod 9$	1 is the multiplicative identity

The final line is the sum of the digits of n, taken modulo 9. Since it is congruent to 0, it is a multiple of 9.

3. Perfect Squares

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.

4. Divisors and Primes

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.