Solutions to In-Class Problems Week 8, Wed.

Problem 1. **(a)** Use the Pulverizer to find the inverse of 13 modulo 23 in the range $\{1, \ldots, 22\}$.

Solution. We first use the Pulverizer to find s, t such that $\gcd(23, 13) = s \cdot 23 + t \cdot 13$, namely,

$$1 = 4 \cdot 23 - 7 \cdot 13.$$

This implies that -7 is an inverse of 13 modulo 23.

Here is the Pulverizer calculation:

x	y	$\text{rem}(x, y)$	$=$	$x - q \cdot y$
23	13	10	$=$	$23 - 13$
13	10	3	$=$	$13 - 10$
			$=$	$13 - (23 - 13)$
			$=$	$(-1) \cdot 23 + 2 \cdot 13$
10	3	1	$=$	$10 - 3 \cdot 3$
			$=$	$(23 - 13) - 3 \cdot ((-1) \cdot 23 + 2 \cdot 13))$
			$=$	$\boxed{4 \cdot 23 - 7 \cdot 13}$
3	1	0	$=$	

To get an inverse in the specified range, simply find $\text{rem}(-7, 23)$, namely **16**.

■

(b) Use Fermat's theorem to find the inverse of 13 modulo 23 in the range $\{1, \ldots, 22\}$.

Solution. Since 23 is prime, Fermat's theorem implies $13^{23-2} \cdot 13 \equiv 1 \pmod{23}$ and so $\text{rem}(13^{23-2}, 23)$ is the inverse of 13 in the range $\{1, \ldots, 22\}$. Now using the method of repeated squaring, we have the following congruences modulo 23:

$$\begin{aligned}
13^2 &= 169 \\
&\equiv \text{rem}(169, 23) = 8 \\
\\
13^4 &\equiv 8^2 \\
&= 64 \\
&\equiv \text{rem}(64, 23) = 18 \\
\\
13^8 &\equiv 18^2 \\
&= 324 \\
&\equiv \text{rem}(324, 23) = 2 \\
\\
13^{16} &\equiv 2^2 \\
&= 4 \\
\\
13^{21} &= 13^{16} \cdot 13^4 \cdot 13 \\
&\equiv 4 \cdot 18 \cdot 13 \\
&= (4 \cdot 6) \cdot (3 \cdot 13) \\
&= 24 \cdot 39 \\
&\equiv 1 \cdot 39 \\
&\equiv \text{rem}(39, 23) = \boxed{16}.
\end{aligned}$$

■

Problem 2. **(a)** Why is a number written in decimal evenly divisible by 9 if and only if the sum of its digits is a multiple of 9? *Hint:* $10 \equiv 1 \pmod 9$.

Solution. Since $10 \equiv 1 \pmod 9$, so is

$$10^k \equiv 1^k \equiv 1 \pmod 9. \tag{1}$$

Now a number in decimal has the form:

$$d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0.$$

From (1), we have

$$d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0 \quad \equiv \quad d_k + d_{k-1} + \ldots + d_1 + d_0 \pmod 9$$

This shows something stronger than what we were asked to show, namely, it shows that the remainder when the original number is divided by 9 is equal to the remainder when the sum of the digits is divided by 9. In particular, if one is zero, then so is the other. ■

(b) Take a big number, such as 37273761261. Sum the digits, where every other one is negated:

$$3 + (-7) + 2 + (-7) + 3 + (-7) + 6 + (-1) + 2 + (-6) + 1 = -11$$

Explain why the original number is a multiple of 11 if and only if this sum is a multiple of 11.

Solution. A number in decimal has the form:

$$d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0$$

Observing that $10 \equiv -1 \pmod{11}$, we know:

$$\begin{aligned}
&d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \cdots + d_1 \cdot 10 + d_0 \\
&\equiv d_k \cdot (-1)^k + d_{k-1} \cdot (-1)^{k-1} + \cdots + d_1 \cdot (-1)^1 + d_0 \cdot (-1)^0 \pmod{11} \\
&\equiv d_k - d_{k-1} + \cdots - d_1 + d_0 \pmod{11}
\end{aligned}$$

assuming k is even. The case where k is odd is the same with signs reversed.

The procedure given in the problem computes $\pm$ this alternating sum of digits, and hence yields a number divisible by 11 ($\equiv 0 \pmod{11}$) iff the original number was divisible by 11. ■

Problem 3.
The following properties of equivalence mod n follow directly from its definition and simple properties of divisibility. See if you can prove them without looking up the proofs in the text.

(a) If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$.

Solution. The condition $a \equiv b \pmod{n}$ is equivalent to the assertion $n \mid (a - b)$. This implies that $n \mid (a - b)c$, and so $n \mid (ac - bc)$. This is equivalent to $ac \equiv bc \pmod{n}$. ■

(b) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Solution. Assume $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, that is, $n \mid (a - b)$ and $n \mid (b - c)$. Then $n \mid (a - b) + (b - c) = (a - c)$, so $a \equiv c \pmod{n}$. ■

(c) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

Solution. $a \equiv b \pmod{n}$ implies $ac \equiv bc \pmod{n}$ by part (a); likewise, $c \equiv d \pmod{n}$ implies $bc \equiv bd \pmod{n}$. So $ac \equiv bd \pmod{n}$ by part (b). ■

(d) $\text{rem}(a, n) \equiv a \pmod{n}$.

Solution. The remainder $\text{rem}(a, n)$ is equal to $a - qn$ for some integer q. However, for every integer q:

$$\begin{aligned}
n \mid qn \quad &\text{IFF} \quad n \mid ((a - qn) - a) \\
&\text{IMPLIES} \quad n \mid (\text{rem}(a, n) - a) \\
&\text{IFF} \quad \text{rem}(a, n) \equiv a \pmod{n}.
\end{aligned}$$

■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010