Problem Set 4 Solutions

Due: Monday, February 28 at 9 PM

Problem 1. Prove all of the following statements except for the two that are false; for those, provide counterexamples. Assume $n > 1$. When proving each statement, you may assume all its predecessors.

(a) $a \equiv a \pmod{n}$

Solution. Every number divides zero, so $n \mid (a - a)$, which means $a \equiv a \pmod{n}$.

(b) $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$

Solution. The statement $a \equiv b \pmod{n}$ implies $n \mid (a - b)$, which means there is an integer k such that $nk = a - b$. Thus, $n(-k) = b - a$, so $n \mid (b - a)$ as well. This means $b \equiv a \pmod{n}$.

(c) $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ implies $a \equiv c \pmod{n}$

Solution. The two assumptions imply $n \mid (a - b)$ and $n \mid (b - c)$. Thus, n divides the linear combination $(a - b) + (b - c) = a - c$ as well. This means $n \mid (a - c)$.

(d) $a \equiv b \pmod{n}$ implies $a + c \equiv b + c \pmod{n}$

Solution. The first statement implies $n \mid (a - b)$. Rewriting the right side gives $n \mid (a + c) - (b + c)$, which means $a + c \equiv b + c \pmod{n}$.

(e) $a \equiv b \pmod{n}$ implies $ac \equiv bc \pmod{n}$

Solution. The first statement implies $n \mid (a-b)$. Thus, n also divides $c(a-b) = ac-bc$. Therefore, $ac \equiv bc \pmod{n}$.

(f) $ac \equiv bc \pmod{n}$ implies $a \equiv b \pmod{n}$ provided $c \not\equiv 0 \pmod{n}$.

Solution. This is false. For example, $6 \cdot 2 \equiv 8 \cdot 2 \pmod{4}$, but $6 \not\equiv 8 \pmod{4}$.

(g) $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ imply $a + c \equiv b + d \pmod{n}$

Solution. The assumptions, together with part (e), give:

$$\begin{aligned} a + c &\equiv b + c \pmod{n} \\ b + c &\equiv b + d \pmod{n} \end{aligned}$$

Now part (c) implies $a + c \equiv b + d \pmod{n}$.

(h) $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ imply $ac \equiv bd \pmod{n}$

Solution. The assumptions, together with part (e), give:

$$\begin{aligned} ac &\equiv bc \pmod{n} \\ bc &\equiv bd \pmod{n} \end{aligned}$$

Now part (c) implies $ac \equiv bc \pmod{n}$.

(i) $a \equiv b \pmod{n}$ implies $a^k \equiv b^k \pmod{n}$ for all $k \geq 0$.

Solution. We use induction. Suppose that $a \equiv b \pmod{n}$. Let $P(k)$ be the proposition that $a^k \equiv b^k$.

Base case. $P(0)$ is true, since $a^0 = b^0 = 1$ and $1 \equiv 1 \pmod{n}$ by part (a).

Inductive step. For $k \geq 0$, we assume $P(k)$ to prove $P(k+1)$. Thus, assume $a^k \equiv b^k \pmod{n}$. Combining this assmption and the fact that $a \equiv b \pmod{n}$ using part (g), we get $a^{k+1} \equiv b^{k+1} \pmod{n}$.

By induction, $P(k)$ holds for all $k \geq 0$.

(j) $a \equiv b \pmod{n}$ implies $k^a \equiv k^b \pmod{n}$ for all $k \geq 0$.

Solution. This is false. For example, $0 \equiv 3 \pmod{3}$, but $2^0 \not\equiv 2^3 \pmod{3}$.

(k) $(a \text{ rem } n) \equiv a \pmod{n}$

Solution. By definition of rem, $a \text{ rem } n = a - qn$ for some integer q. So we can reason as follows:

$$\begin{aligned} (a \text{ rem } n) &\equiv a - qn \pmod{n} \\ &\equiv a \pmod{n} \qquad\qquad \text{from (d) and } qn \equiv 0 \pmod{n} \end{aligned}$$

Problem 2. Prove that there exists an integer k^{-1} such that

$$k \cdot k^{-1} \equiv 1 \pmod{n}$$

provided $\gcd(k, n) = 1$. Assume $n > 1$.

Solution. If $\gcd(k, n) = 1$, then there exist integers x and y such that $kx + yn = 1$. Therefore, $yn = 1 - kx$, which means $n \mid (1 - kx)$ and so $kx \equiv 1 \pmod{n}$. Let k^{-1} be x.

Problem 3. Reviewing the analysis of RSA may help you solve the following problems. You may assume results proved in recitation.

(a) Let n be a nonnegative integer. Prove that n and n^5 have the same last digit. For example:

$$\underline{2}^5 = 3\underline{2} \qquad\qquad 7\underline{9}^5 = 307705639\underline{9}$$

Solution. The correctness of RSA relies on the following fact: if p and q are distinct primes, then

$$m^{1+k(p-1)(q-1)} \equiv m \pmod{pq}$$

for all m and k. Setting $k = 1$, $p = 5$, and $q = 2$ proves the claim.

(b) Suppose that $p_1, \ldots, p_k$ are distinct primes. Prove that

$$m^{1+(p_1-1)(p_2-1)\cdots(p_k-1)} \equiv m \pmod{p_1 p_2 \cdots p_k}$$

for all m and all $k \geq 1$.

Solution. If m is a multiple of a prime p_j, then

$$m^{1+(p_1-1)(p_2-1)\cdots(p_k-1)} \equiv m \pmod{p_j} \tag{*}$$

holds, because both sides are congruent to 0. If m is not a multiple of p_j, then congruence (*) still holds because:

$$\begin{aligned} m^{1+(p_1-1)(p_2-1)\cdots(p_k-1)} &\equiv m \cdot \left(m^{p_j-1}\right)^{(p_1-1)(p_2-1)\cdots(p_k-1)/(p_j-1)} \pmod{p_j} \\ &\equiv m \cdot 1^{(p_1-1)(p_2-1)\cdots(p_k-1)/(p_j-1)} \pmod{p_j} \\ &\equiv m \pmod{p_j} \end{aligned}$$

The second step uses Fermat's Theorem. Now the congruence (*) means that:

$$p_j \mid m^{1+(p_1-1)(p_2-1)\cdots(p_k-1)} - m$$

Thus, p_j appears in the prime factorization of right side. Since this argument is valid for every prime p_j where $1 \leq j \leq k$, all of the primes $p_1, \ldots, p_k$ appear in the prime factorization of:

$$m^{1+(p_1-1)(p_2-1)\cdots(p_k-1)} - m$$

Therefore:

$$p_1 p_2 \cdots p_k \mid m^{1+(p_1-1)(p_2-1)\cdots(p_k-1)} - m$$

Rewriting this as a congruence gives:

$$m^{1+(p_1-1)(p_2-1)\cdots(p_k-1)} \equiv m \pmod{p_1 p_2 \cdots p_k}$$

Problem 4. Suppose that p is a prime.

(a) An integer k is *self-inverse* if $k \cdot k \equiv 1 \pmod{p}$. Find all integers that are self-inverse mod p.

Solution. The congruence holds if and only if $p \mid k^2 - 1$ which is equivalent to $p \mid (k+1)(k-1)$. this holds if and only if either $p \mid k+1$ or $p \mid k-1$. Thus, $k \equiv \pm 1 \pmod{p}$.

(b) *Wilson's Theorem* says that $(p-1)! \equiv -1 \pmod{p}$. The English mathematician Edward Waring said that this statement would probably be extremely difficult to prove because no one had even devised an adequate notation for dealing with primes. (Gauss proved it while standing.) Your turn! Stand up, if you like, and try cancelling terms of $(p-1)!$ in pairs.

Solution. If $p = 2$, then the theorem holds, because $1! \equiv -1 \pmod{2}$. If $p > 2$, then $p-1$ and 1 are distinct terms in the product $1 \cdot 2 \cdot \cdots \cdot (p-1)$, and these are the only self-inverses. Consequently, we can pair each of the remaining terms with its multiplicative inverse. Since the product of a number and its inverse is congruent to 1, all of these remaining terms cancel. Therefore, we have:

$$\begin{aligned}(p-1)! &\equiv 1 \cdot (p-1) \pmod{p} \\ &\equiv -1 \pmod{p}\end{aligned}$$