MATH 3070
Assignment # 3 Solutions
Due Thursday, October 2, 2008

1. Solution 1: Since a and b are invertible, we find that $(ab)(b^{-1}a^{-1}) \equiv 1 \pmod{m}$ so that $(ab)^{-1}$ exists and is equal to $b^{-1}a^{-1}$.

   Solution 2: Since a and b are both invertible, we have that $(a,m) = (b,m) = 1$. If ab is not invertible, then $(ab,m) = d > 1$ so there is a prime p such that $p|ab$ and $p|m$. But by Euclid, $p|ab$ implies $p|a$ or $p|b$ and in either case will be a common facto with m, contradicting invertibility of a or b.

2. If there is a solution to x such that $x^2 \equiv 244714 \pmod{1256636}$, then since $1256636 = 4 \cdot 314159$ by the Chinese Remainder Theorem it must satisfy both $x^2 \equiv 244714 \pmod{4}$ and $x^2 \equiv 244714 \pmod{314159}$ simultaneously. But $244714 \equiv 2 \pmod{4}$ and thus $x^2 \equiv 2 \pmod{4}$, which is impossible since the squares mod 4 are 0 and 1.

3. Let a and m be as in the statement of the problem. The set $S = \{ax : 0 \leq x \leq m-1\}$ contains exactly m elements. Thus by Corollary 13.1 the set is a complete residue system if we can prove that the elements are pairwise incongruent mod m. But that is easy, since if we have two elements ax_1 and ax_2 in S, then $ax_1 \equiv ax_2 \pmod{m}$ implies $x_1 \equiv x_2 \pmod{m}$ since we can cancel the a. Thus the elements of S are pairwise incongruent mod m.

4. (a) Solving the individual congruences, we find that the system is equivalent to

$$\begin{aligned} x &\equiv -1 \pmod{7} \\ x &\equiv -1 \pmod{8} \\ x &\equiv -1 \pmod{29}. \end{aligned}$$

   Thus we find that $x \equiv -1 \pmod{7 \cdot 8 \cdot 29}$.

   (b) Break up the first congruence into prime powers, so $5x \equiv 3 \pmod{12}$ is the same as the system $5x \equiv 3 \pmod{3}$ and $5x \equiv 3 \pmod{4}$. But this means x must satisfy $x \equiv 3 \pmod{4}$. Solving the mod 8 congruence we find that $x \equiv 5 \pmod{8}$. This contradicts the mod 4 congruence. So the system has no solutions.

5. (a) Let $m = 8$, then $x^2 \equiv 1 \pmod{8}$ has solutions $x \equiv 1, 3, 5, 7 \pmod{8}$.

   (b) Suppose $x^2 \equiv a \pmod{p^2}$ has a solution $x \equiv r \pmod{p^2}$. Then we may rewrite the congruence as $x^2 \equiv r^2 \pmod{p^2}$, and any other solution must satisfy $(x+r)(x-r) \equiv 0 \pmod{p^2}$. Thus we have

$$p^2 | (x+r)(x-r).$$

   We have three cases.
   Case 1: $p^2 | (x+r)$, then we have the solution $x \equiv -r \pmod{p^2}$.
   Case 2: $p^2 | (x-r)$, then we have the solution $x \equiv r \pmod{p^2}$.
   Case 3: $p | (x+r)$ and $p | (x-r)$. Then we have the system of simultaneous congruences

$$\begin{aligned} x &\equiv r \pmod{p} \\ x &\equiv -r \pmod{p}. \end{aligned}$$

But since p is an odd prime, $r \not\equiv -r \pmod{p}$ if $r \not\equiv 0 \pmod{p}$. So case 3 has no solutions unless $r \equiv 0 \pmod{p}$. But if $r \equiv 0$, then r^2 has contains a factor of p^2 so $a \equiv 0 \pmod{p^2}$.

(c) Again, we suppose there is a solution $x \equiv r \pmod{p_1p_2}$. Then we use it to find all the other solutions. So any other solution must satisfy

$$p_1p_2|(x+r)(x-r).$$

Here we have four cases.
Case 1: $p_1p_2|(x+r)$, then there is one solution $x \equiv -r \pmod{p_1p_2}$.
Case 2: $p_1p_2|(x-r)$, then there is one solution $x \equiv r \pmod{p_1p_2}$.
Case 3: $p_1|(x+r)$ and $p_2|(x-r)$. This corresponds to the system

$$\begin{aligned} x &\equiv -r \pmod{p_1} \\ x &\equiv r \pmod{p_2}, \end{aligned}$$

which has a unique solution mod p_1p_2 by the Chinese Remainder Theorem.
Case 4: $p_1|(x-r)$ and $p_2|(x+r)$. This corresponds to a system similar to Case 3, and has a unique solution mod p_1p_2 as well.

Since each case yields at most one solution, we obtain a maximum of 4 distinct solutions mod p_1p_2.

6. Since 17 is prime, we apply Fermat's little Theorem to find that if $n \not\equiv 0 \pmod{17}$, then $n^{16} \equiv 1 \pmod{17}$. Thus

$$\begin{aligned} n^{35} - 4n^{24} + 5n^{16} + 21n^8 - n^3 + 2 &= (n^{16})^2n^3 - 4n^{16}n^8 + 5n^{16} + 4n^8 - n^3 + 2 \\ &\equiv n^3 - 4n^8 + 5 + 4n^8 - n^3 + 2 \equiv 7 \pmod{17} \end{aligned}$$

is never zero. If $n \equiv 0 \pmod{17}$, then the polynomial is congruent to $2 \pmod{17}$ which is also not zero.

7. Let n be composite. Then it must have a prime factor p such that $1 < p < n$. Therefore, $n/p \in \mathbb{N}$ and $1 < n/p < n$ as well. So if $p \neq n/p$ then both p and n/p occur in the list $1, 2, \ldots, n-1$ and their product occurs as a factor in $(n-1)!$. Thus $(n-1)! \equiv 0 \pmod{n}$.

On the other hand, if $p = n/p$ then $n = p^2$. If $n > 4$, then $p > 2$ so p and $2p$ are both in the list, since $2p < p^2$, and we also have $(n-1)! \equiv 0 \pmod{n}$.

In the final case, if $n = 4$, then $(n-1)! = 6 \equiv 2 \pmod{4}$.