MATH 25 MIDTERM 2 SOLUTIONS

(1) Find all integers x which simultaneously solve the following congruences:

$$x \equiv 1 \bmod 4, x \equiv 2 \bmod 5, x \equiv 1 \bmod 9.$$

Solution. Because the moduli $4, 5, 9$ are mutually coprime, the Chinese Remainder Theorem guarantees there will be exactly one solution mod $4 \cdot 5 \cdot 9 = 180$. We now find this solution.

First, if $x \equiv 2 \bmod 5$, then $x \equiv 2, 7, 12, 17 \bmod 20$, and the only of these four choices which is $\equiv 1 \bmod 4$ is $17 \bmod 20$. Then we find a solution to $x \equiv 17 \bmod 20, x \equiv 1 \bmod 9$, and quick inspection shows that $37 \bmod 180$ is the solution we are looking for. □

(2) Find all integers x which simultaneously solve the following congruences:

$$x \equiv 22 \bmod 28, x \equiv -2 \bmod 40, 9x \equiv 2 \bmod 35.$$

Solution. This time, because the moduli are not mutually coprime, we cannot yet apply the CRT. Instead, we will break each congruence up into prime power pieces, sort the pieces by prime power, and then use the CRT.

The first congruence is equivalent to $x \equiv 22 \equiv 1 \bmod 7, x \equiv 22 \equiv 2 \bmod 4$. The second congruence is equivalent to $x \equiv -2 \equiv 3 \bmod 5, x \equiv -2 \equiv 6 \bmod 8$. Finally, the last congruence is equivalent to $9x \equiv 2 \bmod 5, 9x \equiv 2 \bmod 7$, which in turn are equivalent to $x \equiv 3 \bmod 5, x \equiv 1 \bmod 7$. (We use $9 \equiv -1 \bmod 5, 9 \equiv 2 \bmod 7$ respectively.)

Now we sort the congruences by prime power. We get the following list, where the congruences in each row have moduli which are powers of the same prime:

$$\begin{aligned} x \equiv 2 \bmod 4, x &\equiv 6 \bmod 8, \\ x &\equiv 3 \bmod 5, \\ x &\equiv 1 \bmod 7. \end{aligned}$$

The first pair of congruences is equivalent to $x \equiv 6 \bmod 8$. So we want to simultaneously solve $x \equiv 6 \bmod 8, x \equiv 3 \bmod 5, x \equiv 1 \bmod 7$, and now we can use the CRT to guarantee that there is exactly one solution mod $5 \cdot 7 \cdot 8 = 280$, since $5, 7, 8$ are mutually coprime.

First consider $x \equiv 6 \bmod 8, x \equiv 3 \bmod 5$. Since $x \equiv 6 \bmod 8$ implies $x \equiv 6, 14, 22, 30, 38 \bmod 40$, and the only of these five classes which is $3 \bmod 5$ is $38 \bmod 40$, these two congruences are equivalent to $x \equiv 38 \bmod 40$. We now add in $x \equiv 1 \bmod 7$, and we find that $x \equiv 78 \bmod 280$ solves $x \equiv 38 \bmod 40$ and $x \equiv 1 \bmod 7$. Therefore $x \equiv 78 \bmod 280$ solves the initial system of congruences. □

(3) Find all integers x which solve the following congruence:

$$x^3 - x + 1 \equiv 0 \bmod 49.$$

Solution. We first find solutions mod 7, and then apply Hensel's Lemma. To solve this congruence modulo 7 we use trial and error, with the proviso that instead of testing $x = 4, 5, 6$, we instead test $x = -3, -2, -1$, since this will keep all numbers which appear small. In the chart, $f(x) = x^3 - x + 1$.

x	-3	-2	-1	0	1	2	3
$f(x)$	-23	-5	1	1	1	7	25

This table makes it clear that the only solution to $x^3 - x + 1 \equiv 0 \bmod 7$ only has solution $x \equiv 2 \bmod 7$.

We now use Hensel's Lemma to determine all lifts of $x \equiv 2 \bmod 7$ which are solutions to $x^3 - x + 1 \equiv 0 \bmod 49$, and because $x \equiv 2 \bmod 7$ is the only solution of the congruence mod 7, these lifts will be all the solutions to the original solution. First, $f'(x) = 3x^2 - 1$, so $f'(2) = 11$, which is not divisible by 7. Therefore Hensel's Lemma tells us that exactly one lift of 2 mod 7 to mod 49 will be a solution to $f(x) \equiv 0 \bmod 49$. We can either find it by brute force (which is rather painful, involving cubing two digit numbers), or use the method of Hensel's Lemma to find the solution.

Recall that Hensel's Lemma tells us that we should try to solve $q_1 + f'(2)k \equiv 0 \bmod 7$, where $q_1 p = f(2)$, for k. Then the solution will be given by $2 + 7k \bmod 49$. Since $f(2) = 7 = 7 \cdot 1$, we have $q_1 = 1$, and $f'(2) \equiv 4 \bmod 7$, so we want to solve $1 + 4k \equiv 0 \bmod 7$. This has solution $k = 5$, so $2 + 35 = 37 \bmod 49$ is the only solution to the congruence $x^3 - x + 1 \equiv 0 \bmod 49$. □

(4) Find all positive integers n which solve

$$\phi(n) = \frac{n}{3}.$$

(ϕ denotes the Euler totient function.)

Solution. Let $n = p_1^{e_1} \dots p_r^{e_r}$ be the prime factorization of n. Then one of the standard formulas for ϕ says that

$$\phi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{r} \frac{p_i - 1}{p_i}.$$

Therefore $\phi(n) = \frac{n}{3}$ is equivalent to

$$\frac{1}{3} = \prod \frac{p_i - 1}{p_i} \Leftrightarrow \prod p_i = 3 \prod (p_i - 1).$$

(From now on the indexing on the products will be assumed to be from $i = 1$ to r unless otherwise mentioned.) First, notice that everything is now a product of integers. Since 3 divides the right hand side of the last equation, it must also divide the left, and because 3 is a prime, Euclid's Lemma says that $3 = p_k$ for some p_k. So $3 \mid n$. But then $p_k - 1 = 2$ appears on the right hand side as well, so 2 divides the right hand side, so that some $p_j = 2$. So $2 \mid n$. We claim that no other primes divide n.

Indeed, notice that if $2, 3 \mid n$, then already

$$\phi(n) = n \cdot \frac{1}{2} \cdot \frac{2}{3} \prod \left(1 - \frac{1}{p_i}\right) = \frac{n}{3} \prod \left(1 - \frac{1}{p_i}\right),$$

where the product is now over all prime divisors of n not equal to $2, 3$ (and is possibly an empty product). Since each term in this product is < 1, the only way $\phi(n) = n/3$ is if the product is equal to 1, and therefore must be empty. This

means that $2, 3$ are the only prime divisors of n, and of course any number of the form $n = 2^a 3^b, a, b > 0$ satisfies $\phi(n) = n/3$. So the solutions of $\phi(n) = n/3$ are the numbers $n = 2^a 3^b, a, b > 0$, or equivalently, any number with exactly $2, 3$ as its prime divisors. □

(5) In this question, you will be given the result of various calculations. On the basis of those calculations, decide whether a certain number is prime, composite, or there is not enough information to decide given what we have learned in this class, and explain why your answer is correct.

(a) $3^{73866} \equiv 1 \bmod 73867$. Is $n = 73867$ prime, composite, or do you not have enough information to decide?

Solution. Not enough information. There is the possibility that 73867 is a base 3 Fermat pseudoprime. (As a matter of fact, 73867 is prime, but there is no obvious short way to compute this by hand.)

(b) The (multiplicative) order of 2 mod 24797 is 3060. Is $n = 24797$ prime, composite, or do you not have enough information to decide?

Solution. You have enough information to decide that $n = 24797$ is composite. Indeed, if $n = 24797$ were prime, then Fermat's Little Theorem tells us that $3060 \mid (n-1) = 24796$. But this evidently is not the case, since $3060 \cdot 8 = 24480$, so clearly $3060 \nmid 24796$.

(c) $7^{1761} \equiv 2711 \bmod 14089, 7^{1761 \cdot 2} \equiv 9162 \bmod 14089, 7^{1761 \cdot 4} \equiv -1 \bmod 14089, 7^{1761 \cdot 8} = 7^{14088} \equiv 1 \bmod 14089$. Is $n = 14089$ prime, composite, or do you not have enough information to decide? (Notice that $1761 \cdot 8 = 14088$.)

Solution. You do not have enough information to decide. The information given is enough to run a modified Fermat compositeness test (sometimes called a single run of Miller-Rabin), and this number passes this test, so that the test is inconclusive. As a matter of fact, $14089 = 73 \cdot 193$, so is composite.

(d) $2^{6873} \equiv 9321 \bmod 13747, 2^{13746} \equiv 1 \bmod 13747$. Is $n = 13747$ prime, composite, or do you not have enough information to decide? (Notice that $6873 \cdot 2 = 13746$.)

Solution. Again, this is enough information to run a modified Fermat compositeness test, and in this case the test shows that 13747 is composite, because $2^{6873} \not\equiv \pm 1 \bmod 13747$. As a matter of fact, even if you had forgotten this test, you could have still figured this out, because if $n = 13747$ were prime, then $x^2 \equiv 1 \bmod n$ should only have the two solutions $x \equiv \pm 1 \bmod n$, but the calculations above show that $x \equiv 9321 \bmod 13747$ is a third solution. Notice that none of this actually gives you any factors of 13747, but one can compute $13747 = 59 \cdot 233$ by trial division or other methods. □

(6) Let $p > 2$ be an odd prime. Recall that a *complete residue system* of U_p is a set of $p-1$ integers $r_1, \ldots, r_{p-1}$ such that these $p-1$ integers are in $p-1$ different nonzero congruence classes mod p.

If $r_1, \ldots, r_{p-1}$ and $r'_1, \ldots, r'_{p-1}$ are two complete residue systems of U_p, show that $r_1 r'_1, \ldots, r_{p-1} r'_{p-1}$ is not a complete residue system of U_p. (Hint: Wilson's Theorem says that $(p-1)! \equiv -1 \bmod p$.)

Solution. Let $r_1, \ldots, r_{p-1}$ be any complete residue system of U_p. Then considered as classes mod p, these are a permutation of the classes $1, 2, \ldots, p-1 \bmod p$. Therefore

$$r_1 \cdot r_2 \cdot \ldots \cdot r_{p-1} \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) = (p-1)! \bmod p.$$

By Wilson's Theorem this entire expression is $-1 \bmod p$. So we have shown that the product of all the elements of a complete residue system of U_p is congruent to $-1 \bmod p$.

Now consider $r_1 r_1', \ldots, r_{p-1} r_{p-1}'$. Their product mod p is

$$r_1 r_1' \ldots r_{p-1} r_{p-1}' \equiv (r_1 \ldots r_{p-1})(r_1' \ldots r_{p-1}') \equiv (-1)(-1) \equiv 1 \bmod p.$$

However because $p > 2$, we have $1 \not\equiv -1 \bmod p$, so this shows that $r_1 r_1', \ldots, r_{p-1} r_{p-1}'$ cannot be a complete residue system of U_p because their product is not congruent to $-1 \bmod p$. $\square$