Homework 7 Solutions

Tim Smits

1. Let p be a prime. Prove that if $a^2 \equiv 1 \bmod p$, then $a \equiv 1 \bmod p$ or $a \equiv -1 \bmod p$.

Solution: If $a^2 \equiv 1 \bmod p$, this says $p \mid a^2 - 1 = (a-1)(a+1)$. Since p is prime, Euclid's lemma says $p \mid (a-1)$ or $p \mid (a+1)$, i.e. $a \equiv 1 \bmod p$ or $a \equiv -1 \bmod p$.

2.

(a) Reduce $(p-1)! \bmod p$ for $p = 2, 3, 5, 7, 11$.

(b) Prove that if p is prime, that $(p-1)! \equiv -1 \bmod p$.

Solution:

(a) They all reduce to $-1 \bmod p$.

(b) This is trivial for $p = 2, 3$ so let $p \geq 5$. Since p is is prime, each integer $2 \leq x \leq p-2$ is invertible mod p. Further, problem 1 says the only residue classes that are their own inverse mod p are $1 \bmod p$ and $-1 \bmod p$. Therefore, for each integer $2 \leq x \leq p-2$, the residue class $x \bmod p$ has as an inverse some other distinct residue class $y \bmod p$ for some integer $2 \leq y \leq p-2$. Since there are $p-3$ integers in this range and this number is even, each residue class pairs up with an inverse, so we see that $2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1 \bmod p$. This then says $(p-1)! \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv 1 \cdot (p-1) \equiv -1 \bmod p$.

3. For $n = 4, 6, 8, 9$, reduce $(n-1)! \bmod n$. Then prove that $(n-1)! \equiv 0 \bmod n$ for all composite $n \geq 4$.

Solution: $(n-1)! \equiv 0 \bmod n$ for $n = 6, 8, 9$ and $(n-1) \equiv 2 \bmod n$ for $n = 4$.

To prove the result, this is equivalent to showing that $n \mid (n-1)!$, which is how we will approach the problem. Firstly, it's sufficient to check that if some prime power $p^e \mid\mid n$ that $p^e \mid (n-1)!$, because then by unique factorization, all the prime powers in the factorization of n divide $(n-1)!$, so that $n \mid (n-1)!$. If n is not a prime power, then p^e is a non-trivial divisor of n, and therefore $p^e < n$ so that p^e appears as one of the terms in $(n-1)!$, and so we are immediately done. If $n = p^e$ is a prime power for some $e \geq 2$, we need there to be enough multiples of p appearing as terms in $(p^e-1)!$. Note that $p, p^2, \ldots, p^{e-1}$ are all terms that appear as terms in $(p^e-1)!$, so if $e > 2$ we have at least $1 + 2 + \ldots + (e-1) = \frac{e(e-1)}{2}$ copies of p appearing, and $\frac{e(e-1)}{2} \geq e$ for $e > 2$, so we are good. The last case we have to handle is if $e = 2$. In this case, $n = p^2$, so we need some other multiple of p to divide $(p^2-1)!$. We see that $2p < p^2 - 1$ for all $p > 2$, so we are good. This leaves the only exceptional case as $n = 2^2 = 4$, in which case we saw the result is not true.

4. Suppose you know the following: $(1552756)! \equiv -1 \bmod 1552757$, $(1479406)! \equiv 0 \bmod 1479407$, $(5016358)! \equiv 0 \bmod 5016359$ and $(6424992)! \equiv -1 \bmod 6424993$. Which numbers are prime and which are composite?

Solution: By the previous two problems, we can say that 1552757 and 6424993 are prime, while 1479407 and 5016359 are composite.

5. The following exercise is a primality test based on Fermat's little theorem.

(a) If $2^{5733348} \equiv 5408246 \bmod 5733349$, can you determine from this if 5733349 is prime or composite?

(b) If $5^{3163128} \equiv 1706983 \bmod 3163129$, can you determine from this if 3163129 is prime or composite?

(c) If $3^{2182020} \equiv 1 \bmod 2182021$, can you determine from this if 2182021 is prime or composite?

(d) If $2^{340560} \equiv 1 \bmod 340561$, $3^{340560} \equiv 1 \bmod 340561$, $5^{340560} \equiv 1 \bmod 340561$, and $7^{340560} \equiv 1 \bmod 340561$, can you determine from this if 340561 is prime or composite?

(e) Can this primality test give false negatives? False positives? For the numbers where the test didn't tell you if the number was prime or not, check with a computer to see if they are.

Solution:

(a) This is not prime by the contrapositive of Fermat's little theorem.

(b) This is also not prime by the same reasoning.

(c) We cannot determine if this number is prime or not from Fermat's little theorem alone.

(d) Same as above, the extra congruence information does not tell us anything.

(e) The point is that Fermat's little theorem cannot give false negatives if $a^n \not\equiv 1 \bmod n$, then n is necessarily composite. However, it *can* give false negatives, e.g. 340561.

6. Compute the following:

(a) $\varphi(75)$

(b) $\varphi(360)$

(c) $\varphi(7000)$

(d) $\varphi(22041360)$ where $22041360 = 2^4 \cdot 3^2 \cdot 5 \cdot 11^3 \cdot 23$

Solution: Use the formula $\varphi(n) = n \prod_{p|n}(1 - \frac{1}{p})$.

(a) $\varphi(75) = 40$.

(b) $\varphi(360) = 96$.

(c) $\varphi(7000) = 2400$.

(d) $\varphi(22041360) = 5111040$.

7. Reduce the following mod n.

(a) $43^{1250} \bmod 360$

(b) $21002^{12012} \bmod 7000$

(c) $5^{4819710726} \bmod 22041360$

Solution:

(a) By Euler's theorem, $43^{96} \equiv 1 \bmod 360$. Then $1250 \equiv 2 \bmod 96$, so $43^{1250} \equiv 43^2 \equiv 49 \bmod 360$.

(b) Since $7000 = 2^3 \cdot 5^3 \cdot 7$, we can reduce 2^{12012} modulo $8, 125$, and 7 and use the Chinese remainder theorem to glue the information back together. Since $2^{12012} \equiv 0 \bmod 8$, $2^{12012} \equiv 96 \bmod 125$, and $2^{12012} \equiv 1 \bmod 7$, (use Euler's theorem to see the second and third relations), this says we are looking for the solution to the system $x \equiv 0 \bmod 8$, $x \equiv 96 \bmod 125$, and $x \equiv 1 \bmod 7$. This is given by $x \equiv 4096 \bmod 7000$, so $2^{12012} \equiv 4096 \bmod 7000$.

(c) We can use the factorization $22041360 = 2^4 \cdot 3^2 \cdot 5 \cdot 11^3 \cdot 23$ and the same method in part (b) to do this computation. The details are more annoying, so they are omitted. Eventually you will find that $5^{4819710726} \bmod 22041360 \equiv 15625 \bmod 22041360$.

8. Reduce $100^{101^{102}} \bmod 13$.

Solution: By first reducing mod 13, we need to compute $9^{101^{102}} \bmod 13$. By Fermat's little theorem, $9^{12} \equiv 1 \bmod 13$, so we need to compute the exponent mod 12. We see $101^{102} \equiv 5^{102} \bmod 12$, and since $\varphi(12) = 4$, this says $5^4 \equiv 1 \bmod 12$ by Euler's theorem. Therefore $5^{102} \equiv 5^2 \equiv 1 \bmod 12$, so that $9^{101^{102}} \equiv 9 \bmod 13$.