Solutions to Homework 7

Tim Smits

February 26, 2022

1. Do the following computations.

(a) Reduce $8263^{12012} \bmod 7000$.

(b) Reduce $100^{101^{102}} \bmod 13$.

(c) Find all primes p such that $\mathrm{ord}_p(2) = 24$.

(d) Solve the equation $x^{13} \equiv 35 \bmod 360$.

Solution:

(a) We have $\varphi(7000) = 2400$, and $8263 \equiv 1263 \bmod 7000$. Euler's theorem tells us exponents only matter mod $\varphi(n)$, so we have $8623^{12012} \equiv 1263^{12} \bmod 7000$. One can then check that $1263^{12} \equiv 4481 \bmod 7000$.

An alternative (better) method is as follows: $7000 = 2^3 \cdot 5^3 \cdot 7$, so the congruence $x \equiv 8263^{12012} \bmod 7000$ is equivalent to the system of congruences $x \equiv 8263^{12012} \bmod 8$, $x \equiv 8263^{12012} \bmod 125$, $x \equiv 8263^{12012} \bmod 7$ by CRT. Reducing each expression using the same idea as the first paragraph, we find $x \equiv 1 \bmod 8, x \equiv 106 \bmod 125, x \equiv 1 \bmod 7$. Solving the system using the methods of the previous homework yields $x \equiv 4481 \bmod 7000$.

(b) We have $\varphi(13) = 12$. Since exponentiation only matters mod $\varphi(n)$, first we need to compute $101^{102} \bmod 12$. We have $101 \equiv 5 \bmod 12$ and $\varphi(12) = 4$, so now the exponent only matters mod 4. Since $102 \equiv 2 \bmod 4$, we find $101^{102} \equiv 5^2 \equiv 1 \bmod 12$. This then says $100^{101^{102}} \equiv 9^1 \equiv 9 \bmod 13$.

(c) Since $\mathrm{ord}_p(2) = 24$, we have $2^{24} \equiv 1 \bmod p$. In particular, we must have $2^{12} \equiv -1 \bmod p$, because $(2^{12})^2 \equiv 1 \bmod p$ and the only solutions to $x^2 \equiv 1 \bmod p$ are $\pm 1 \bmod p$ (and it can't be 1 because otherwise 24 wouldn't be the order!). This says $p \mid 2^{12}+1 = 17 \cdot 241$, so $p = 17$ or $p = 241$ are the only possibilities. On the other hand, by Fermat's little theorem $2^{p-1} \equiv 1 \bmod p$, so $24 = \mathrm{ord}_p(2) \mid p-1$ says $p \equiv 1 \bmod 24$. This means $p = 241$ is the only possibility, and indeed one can check by hand that one actually has $\mathrm{ord}_{241}(2) = 24$.

(d) We wish to find k such that $x^{13k} \equiv x \bmod 360$. Then, we would have $x \equiv 35^k \bmod 360$. Since $\varphi(360) = 96$ and exponentiation only matters mod $\varphi(n)$, we wish to find k such that $13k \equiv 1 \bmod 96$. This is a standard inverse computation, and solving yields $k \equiv 37 \bmod 96$. Plugging in then yields $x \equiv 35^{37} \equiv 35 \bmod 360$.

2. This exercise is a primality test based on Fermat's little theorem. For any integer a and prime p with $p \nmid a$, Fermat's little theorem says $a^{p-1} \equiv 1 \bmod p$, so taking the contrapositive of this statement says that if $a^{p-1} \not\equiv 1 \bmod p$, then p is composite! This gives rise to an algorithm for testing if an integer n is prime or not:

- Randomly pick an integer a with $n \nmid a$.
- If $a^{n-1} \not\equiv 1 \bmod n$, then n is composite and we're done!
- Otherwise, if $a^{n-1} \equiv 1 \bmod n$, pick a different integer a and repeat.

If a is an integer such that $a^{n-1} \not\equiv 1 \bmod n$, we call a a *Fermat witness* for the compositeness of n.

(a) Using WolframAlpha or any other computer algebra system, find the smallest Fermat witness for 2821.

(b) Let $m = 56052361$. Using WolframAlpha or any other computer algebra system, determine if $2, 3, 5, 6, 7, 10$, or 11 are Fermat witnesses for m. What do you find? Is this enough information to tell you with certainty if m is prime or composite, and why?

We call n a *Carmichael number* if $a^{n-1} \equiv 1 \bmod n$ for all integers a with $\gcd(a, n) = 1$. Carmichael numbers are the integers for which our primality test will never give us any information.

(c) Prove that 561 is a Carmichael number. *(Hint:* $561 = 3 \cdot 11 \cdot 17$. *Euler's theorem might be useful.)*

Solution:

(a) Try $a = 2, 3, 5, 6, 7$ on WolframAlpha and you'll find $a = 7$ is the smallest witness.

(b) For all listed values of a, one has $a^{m-1} \equiv 1 \bmod m$. This information isn't enough to tell you anything. It's possible that there's a witness we just haven't found yet, which would mean m is composite. On the other hand, even if we don't find a witness, this doesn't mean anything. The test just says if there is a witness, then m is composite, it can't give us information about whether m is prime.

Remark: 56052361 is actually a Carmichael number, so $a^{m-1} \equiv 1 \bmod m$ for all a coprime to m!

(c) Since $561 = 3 \cdot 11 \cdot 17$, Euler's theorem says for any a coprime to 561 we have $a^2 \equiv 1 \bmod 3$, $a^{10} \equiv 1 \bmod 11$, and $a^{16} \equiv 1 \bmod 17$. Since 560 is divisible by $2, 10, 16$, we have $a^{560} \equiv 1 \bmod 3$, $a^{560} \equiv 1 \bmod 11$, and $a^{560} \equiv 1 \bmod 17$, so gluing together yields $a^{560} \equiv 1 \bmod 561$ as desired.

3. Euler's theorem says for any integer a with $\gcd(a, n) = 1$, that $a^{\varphi(n)} \equiv 1 \bmod n$. However, $\varphi(n)$ is often times not the smallest exponent we can choose with this property. The *Carmichael function* $\lambda(n)$ is defined to be the smallest positive integer k such that $a^k \equiv 1 \bmod n$ for all integers a with $\gcd(a, n) = 1$. It turns out, for example, that $\lambda(1729) = 36$, and so every integer a with $\gcd(a, 1729) = 1$ satisfies $a^{36} \equiv 1 \bmod 1729$.

(a) Prove that n is Carmichael number if and only if $\lambda(n) \mid n - 1$.

(b) Compute $\lambda(3), \lambda(11)$ and $\lambda(17)$.

(c) Compute $\lambda(561)$.

Solution:

(a) First, suppose that $\lambda(n) \mid n-1$, so $n-1 = \lambda(n)k$ for some integer k. Then since $a^{\lambda(n)} \equiv 1 \bmod n$ by definition, we have $a^{n-1} = (a^{\lambda(n)})^k \equiv 1 \bmod n$. Conversely, suppose that n is a Carmichael number, so that $a^{n-1} \equiv 1 \bmod n$ for any a coprime to n. Write $n-1 = \lambda(n)q + r$ with $0 \leq r < \lambda(n)$ by the division algorithm. Then for any a coprime to n, we have $1 \equiv a^{n-1} \equiv (a^{\lambda(n)})^q \cdot a^r \equiv a^r \bmod n$. This forces $r = 0$ because $\lambda(n)$ is the smallest *positive* integer with this property, and so $\lambda(n) \mid n-1$ as desired.

(b) One can check (by hand, for example) that there are generators mod 3, mod 11, and mod 17: 2 is a generator mod 3 and mod 11, while 3 is a generator mod 17. In particular, this means the smallest exponent you can raise said generator to get back 1 in each case is $2, 10, 16$ respectively, which would force $\lambda(3) = 2$, $\lambda(11) = 10$, $\lambda(17) = 16$.

(c) From the previous problem, for any a coprime to 561 we know that $a^2 \equiv 1 \bmod 3$, $a^{10} \equiv 1 \bmod 11$, and $a^{16} \equiv 1 \bmod 17$. The least common multiple of $2, 10, 16$ is 80, and so we have $a^{80} \equiv 1 \bmod 3, 11, 17$ which would tell us $a^{80} \equiv 1 \bmod 561$. In particular, this says $\lambda(561) \leq 80$. The point is that we have *generators* mod $3, 11, 17$, and if g is a generator mod p we have $g^k \equiv 1 \bmod p$ if and only if $p-1 \mid k$. This says $2, 10, 16 \mid \lambda(561)$ and so $\lambda(561)$ is divisible by their least common multiple, which says $80 \mid \lambda(561)$ so $80 \leq \lambda(561)$. This yields $\lambda(561) = 80$.

4. The goal of this problem is to give an alternate proof of Euler's theorem following the main philosophy of number theory.

(a) Prove that for any integer k with $1 \leq k \leq p-1$, that $\binom{p}{k} \equiv 0 \bmod p$.

(b) For any integer $a \geq 0$, prove by induction on a that $a^p \equiv a \bmod p$. Deduce that for $\gcd(a, p) = 1$, that $a^{\varphi(p)} \equiv 1 \bmod p$. (*You may assume the binomial theorem for this.*)

(c) Prove that for any integers a, k with $k \geq 1$ and $\gcd(a, p) = 1$, that $a^{\varphi(p^k)} \equiv 1 \bmod p^k$. (*Again, you may assume the binomial theorem for this.*)

(d) Prove that for integers a, n with $\gcd(a, n) = 1$ that $a^{\varphi(n)} \equiv 1 \bmod n$.

Solution:

(a) By definition, $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. Binomial coefficients are integers, and for $0 \leq k \leq p-1$ the expression in the denominator contains no factor of k because each term in the factorials are less than p. Since there is a factor of p up top, we get $p \mid \binom{p}{k}$ so $\binom{p}{k} \equiv 0 \bmod p$.

(b) This is obvious for $a = 0$. Assume that for some integer k that $k^p \equiv k \bmod p$. We wish to show that $(k+1)^p \equiv k+1 \bmod p$. By the binomial theorem, $(k+1)^p \equiv \sum_{i=0}^{p} \binom{p}{i} k^i \equiv k^p + 1 \equiv k+1 \bmod p$ by assumption, and because all coefficients in the sum except the last two vanish mod p by part (a). This is what we wanted, so we're done by induction.

(c) We prove by induction on k that $a^{\varphi(p^k)} \equiv 1 \bmod p^k$ for $k \geq 1$. The base case $k = 1$ was the previous part. Now assume that $a^{\varphi(p^k)} \equiv 1 \bmod p^k$ for some k. We wish to show that $a^{\varphi(p^{k+1})} \equiv 1 \bmod p^{k+1}$. Note that $\varphi(p^{k+1}) = p\varphi(p^k)$ from the formula $\varphi(p^k) = p^{k-1}(p-1)$. Therefore, $a^{\varphi(p^{k+1})} \equiv a^{p\varphi(p^k)} \equiv (a^{\varphi(p^k)})^p \bmod p^{k+1}$. Since $a^{\varphi(p^k)} \equiv 1 \bmod p^k$ by assumption, we can write $a^{\varphi(p^k)} = 1 + p^k\ell$ for some integer ℓ. Plugging in, we want to compute $(1 + p^k\ell)^p \bmod p^{k+1}$. By the binomial theorem, we have $(1 + p^k\ell)^p \equiv \sum_{i=0}^{p} \binom{p}{i} (p^k\ell)^i \equiv 1 \bmod p^{k+1}$ because $(p^k\ell)^i$ is divisible by p^{k+1} for $2 \leq i \leq p$ and for $i = 1$ we have $\binom{p}{1} = p$ so $p \cdot (p^k\ell)$ is divisible by p^{k+1}. Therefore, we have shown that $a^{\varphi(p^{k+1})} \equiv 1 \bmod p^{k+1}$ and so by induction, we're done.

(d) Write $n = p_1^{e_1} \cdots p_k^{e_k}$ as a product of primes. By part (b), we have $a^{\varphi(p_i^{e_i})} \equiv 1 \bmod p_i^{e_i}$ for all i. Since $\varphi(p_i^{e_i}) \mid \varphi(n)$ for each i, in particular this says $a^{\varphi(n)} \equiv 1 \bmod p_i^{e_i}$ for each i, and gluing back together with CRT says $a^{\varphi(n)} \equiv 1 \bmod n$ as desired.

5. On homework 2, you proved the only integers of the form $2^n - 1$ that can be prime are *Mersenne primes*, primes of the form $2^p - 1$ for prime p, and that the only integers of the form $2^n + 1$ that can be prime are *Fermat numbers*, integers of the form $2^{2^n} + 1$.

(a) Let p be an odd prime, and let q be a prime divisor of $2^p - 1$. Prove that $\mathrm{ord}_q(2) = p$. Similarly, for odd prime p prove that if $p \mid 2^{2^n} + 1$ then $\mathrm{ord}_p(2) = 2^{n+1}$.

(b) Deduce that if q is a prime divisor of $2^p - 1$, then $q = 2pk + 1$ for some integer k. Similarly, deduce that if p is a prime divisor of $2^{2^n} + 1$, that p must be of the form $2^{n+1}k + 1$ for some integer k.

(c) On homework 2, you proved using a computer that $2^{32} + 1 = 641 \cdot 6700417$. Use the previous part to explain how one could identify 641 as a possible factor, and prove by hand that $641 \mid 2^{32} + 1$ using modular arithmetic, so that 641 is the smallest prime divisor of $2^{32} + 1$. Similarly, find by hand the smallest prime divisor of $2^{29} - 1$.

Solution:

(a) We have $2^p \equiv 1 \bmod q$ by assumption, and so this says $\mathrm{ord}_q(2) \mid p$, so $\mathrm{ord}_q(2) = 1$ or p. It's obviously not 1, so $\mathrm{ord}_q(2) = p$ as desired. Similarly, one has $2^{2^n} \equiv -1 \bmod p$, and so squaring yields $2^{2^{n+1}} \equiv 1 \bmod p$. This says $\mathrm{ord}_p(2) \mid 2^{n+1}$. The order must then be 2^k for some $1 \leq k \leq n+1$. If $k < n+1$, write $n = k + r$ for some $r \geq 0$. We then have $2^{2^n} = (2^{2^k})^{2^r}$ and so this would mean that $2^{2^n} \equiv 1 \bmod p$, which is a contradiction. This leaves $\mathrm{ord}_p(2) = 2^{n+1}$ as the only possibility.

(b) From part (a), we showed that $\mathrm{ord}_q(2) = p$. Since $2^{q-1} \equiv 1 \bmod q$ by Fermat's little theorem, this says $p \mid q - 1$. Since q is even, we must also have $2 \mid q - 1$ and so $2p \mid q - 1$, i.e. $q = 1 + 2pk$ for some k. Similarly, $2^{p-1} \equiv 1 \bmod p$ and therefore part (a) says $2^{n+1} \mid p - 1$ yields $p = 1 + 2^{n+1}k$ for some k.

(c) $32 = 2^5$ so any prime factor of $2^{32} + 1$ is of the form $64k + 1$, and 641 is indeed of this form. We then want to show that $2^{32} \equiv -1 \bmod 641$, so that 641 is a factor of $2^{32} + 1$. At this point, this is just a straightforward computation: $2^8 \equiv 256 \bmod 641$ and so $2^{16} \equiv (256)^2 \equiv 154 \bmod 641$ and $2^{32} \equiv (154)^2 \equiv 640 \equiv -1 \bmod 641$.

Similarly, any prime factor of $2^{29} - 1$ must be of the form $1 + 58k$. The first two primes of this form are 59 and 233. We have $2^{25} \equiv (32)^5 \equiv 11 \bmod 59$ so $2^{29} \equiv 11 \cdot 16 \equiv -1 \bmod 59$. Checking 233, we have $2^{25} \equiv (32)^5 \equiv 102 \bmod 233$ and so $2^{29} \equiv 16 \cdot 102 \equiv 1 \bmod 233$, so 233 is the smallest prime dividing $2^{29} - 1$.

6. On homework 4, you proved that there were infinitely many primes of the form $4k + 3$. Now, you will prove that there are infinitely many primes of the form $4k + 1$.

(a) Show that the odd prime divisors of the integer $n^2 + 1$ are of the form $4k + 1$.

(b) Prove there are infinitely many primes of the form $4k + 1$. (*Hint: consider* $(2p_1 \cdots p_k)^2 + 1$.)

Solution:

(a) Let p be an odd prime divisor of n^2+1, so $n^2 \equiv -1 \bmod p$. Then squaring says $n^4 \equiv 1 \bmod p$, so $\text{ord}_p(n) \mid 4$. It's not 2 by what we just said, so $4 = \text{ord}_p(n)$. Note that $p \nmid n$ because otherwise $p \mid (n^2+1) - n^2 = 1$. Therefore, $n^{p-1} \equiv 1 \bmod p$ by Fermat's little theorem and so $4 \mid p-1$ yields $p = 4k+1$ for some k as desired.

(b) Suppose there were finitely many primes $p_1, \ldots, p_k$ with $p_i \equiv 1 \bmod 4$. Consider $N = (2p_1 \cdots p_k)^2 + 1$: we have $N \equiv 1 \bmod 4$, so if it's prime, we've found a new prime that's 1 mod 4, which is a contradiction. Therefore, it must have some prime divisor p. By part (a), $p \equiv 1 \bmod 4$ so $p = p_i$ for some i. However, clearly $N \equiv 1 \bmod p_i$ and so none of the p_i divide N, which also is a contradiction. Therefore, there must be infinitely many primes that are congruent to 1 mod 4.