# Homework 6 Written Solutions

## Written Part

4. In question 2 parts (d) and (e) were similarly sized numbers, yet your algorithm probably only worked on one of them (mine did). Explain why this is (*Hint*: try factoring $p-1$ in sage for the one that worked.)
In part (d), the number 523097775055862871433433884291 factored as $835667525772397 \cdot 625963985584303 = pq$. Then sage factors $p-1$ as $1^2 * 3^2 * 173 * 3323 * 4297 * 9397$. One could also see how many steps it took for Pollards algorithm to run, and we would see that it is precisely 9397. Why did this work? Because 9397! contains all the prime facotrs of $p-1$, so in particular $p-1$ divides 9398!. Therefore $2^{9397!} \equiv 1 \mod p$ by Fermat's little theorem. Since this is the first time this happens (for either $p$ or $q$), it will turn out that $2^{9397!} \not\equiv 1 \mod q$, so that $\gcd(2^{9397!}, pq) = p$ hence the result.

   The upshot here was that $p-1$ had many small prime factors. For the number in part (e), we know it is $p'q'$ for some primes $p'$ and $q'$, but if both $p'-1$ and $q'-1$ have very large prime factors (say in the millions), we would have to get to computing $2^{1000000!} \mod N$, or greater which quickly becomes out of control.

5. Using your data from question 3(d), make a conjecture comparing the number of primes congruent to 1 modulo 4 and the number of primes congruent to 3 modulo 4.
I computed $\pi_1(10^6)/\pi_3(10^6) = 0.9948003327787022$, so it looks like it is approaching 1, so the number of primes congruent to 1 mod 4 is probably about equal to the number of primes congruent to 3 mod 4.

6. Recall the following definition:

   **Definition 1.** *A composite number $n$ is called a Carmichael Number if $a^n \equiv a \mod n$ for every integer $a$.*

   In essense, these are the composite numbers that satisfy Fermat's little theorem. One way you could check if a number $n$ is a Carmichael number is to raise every integer $\leq n$ to the $n$'th power. But it turns out there is some interesting underlying structure to Carmichael numbers making their existence seem less coincidental. Let's explore this:

   (a) We begin by proving that our example 561 from class is a Carmichael number. Notice that $561 = 3 * 11 * 17$. Show that for every $a$ the following congruences hold:

$$\begin{aligned} a^{561} &\equiv a \mod 3 \\ a^{561} &\equiv a \mod 11 \\ a^{561} &\equiv a \mod 17. \end{aligned}$$

   Use this fact to prove that the same congruence holds mod 561 therefore proving that 561 is a Carmichael number.

   *Proof.* If $a$ is divisible by 3, then both $a^{561}$ and $a$ are congruent to 0 mod 3, so they are equal mod 3. Otherwise we know $3 \not| a$. Since $(3-1) = 2$ divides 560, we have $a^{560} \equiv 1 \mod 3$ by Fermat's little theorem so that multiplying both sides by $a$ gives the desired

congruence.

The other 2 congruences are similar. I will spell them out so that we get a sense of the general case. If $a$ is divisible by 11 then both $a^{561}$ and $a$ are 0 mod 11 and the desired congruence holds. Otherwise we know $11 \not| a$. Notice that $11 - 1 = 10$ divides 560 so that $a^{560} \equiv 1 \mod 11$ by Fermat so that multiplying both sides by $a$ gives the desired congruence.

If $a$ is divisible by 17 then both $a^{561}$ and $a$ are 0 mod 17 and the desired congruence holds. Otherwise we know $17 \not| a$. Notice that $17 - 1 = 16$ divides 560 so that $a^{560} \equiv 1 \mod 17$ by Fermat, so that multiplying both sides by $a$ gives the desired congruence.

So we see that all 3 congruences hold modulo 3,11, and 17. In particular, both $a^{561}$ and $a$ solve the congruences:

$$\begin{aligned} x &\equiv a \mod 3 \\ x &\equiv a \mod 11 \\ x &\equiv a \mod 17. \end{aligned}$$

By the uniqueness part of the Chinese Remainder Theorem, we get $a^{561} \equiv a \mod 561$. Since $a$ was arbitrary, we have proved that 561 is a Carmichael number. □

(b) Use the same logic to show that $75361 = 11 * 13 * 17 * 31$ is a Carmichael number.

*Proof.* Rather than repeat the proof we've already written 3 times in part (a), we state a general lemma.

**Lemma 1.** *Let $N = p_1 p_2 \cdots p_n$ be a product of distinct primes. Suppose $(p_i - 1)$ divides $N$ for each $p_i$. Then the following two statements hold.*

*(i) For all $a \in \mathbb{Z}$, $a^N \equiv a \mod p_i$.*

*(ii) For all $a \in \mathbb{Z}$, $a^N \equiv a \mod N$.*

*Proof.* For part (i), fix $p_i$. There are two cases. First assume $a$ is divisible by $p_i$. Then both $a^N$ and $a$ are 0 mod $p_i$ and so the desired congruence holds. Otherwise, we know $p_i \not| a$, so we can use Fermat's little theorem. Indeed, since $p_i - 1 | N - 1$ we see that $a^{N-1} = (a^{p_i - 1})^k$. But the latter is congruent to 1 mod $p_i$ by Fermat's little theorem. Multiplying both sides by $a$ gives the desired congruence.

Part (ii) follows from part (i) by Sun Tzu's theorem. Indeed, part (i) shows that $a^N$ and $a$ are both solutions to the system of congruences:

$$\begin{aligned} x &\equiv a \mod p_1 \\ x &\equiv a \mod p_2 \\ &\vdots \\ x &\equiv a \mod p_n. \end{aligned}$$

By the uniqueness part of the Chinese Remainder theorem then $a^N \equiv a \mod p_1 p_2 \cdots p_n = N$. □

By Lemma 1, to prove that 75361 is a Carmichael number it suffices to show that $10, 12, 16, 30$ all divide 75360, which is easily verified. □

Hopefully we've now noticed a few patterns. Let's extrapolate these to prove some general facts about Carmichael numbers.

(c) Show that a Carmichael number must be odd.

*Proof.* If $N = 2$ then it is prime, and Carmichael numbers are by definition composite. We delay the case where $N = 2^d$ is a power of 2 to part (d), where we show Carmichael numbers must be square free. Therefore what remains is the case where $N$ is an even number with an odd prime factor $p$.

Suppose (for the sake of contradiction) that $N$ is an even number Carmichael number with an odd prime factor $p$, and let $g$ be a primitive root for $\mathbb{F}_p^*$. By assumption we know $g^N \equiv g \mod N$, so that $g^N \equiv g \mod p$. Since $g$ is a unit this implies $g^{N-1} \equiv 1 \mod p$. Since the order of $g$ in $\mathbb{F}_p^*$ is $p-1$ this implies that $p-1$ divides $N-1$. But $p-1$ is even and $N-1$ is odd, and odd numbers are *never* divisible by even numbers. This contradiction shows there are no even numbers Carmichael numbers with odd prime factors. □

(d) Show that a Carmichael number must factor into a product of distinct prime numbers (such a number is called *square free*).

*Proof.* We first point out that if $N$ is not square free, then there exists a prime number $p$ such that $p^2|N$. Indeed, take any $p$ appearing more than once in the prime factorization of $N$. This justifies the terminology.

Suppose (for the sake of contradiction) that $N$ is a Carmichael number and $p$ is a prime with $p^2|N$. Since $N$ is a Carmichael number we see that $p^N \equiv p \mod N$, so that $p^N \equiv p \mod p^2$. But since $N \geq 2$ we know $p^N \equiv 0 \mod p^2$, a contradiction. So $N$ must cannot be divisible by any square and is therefore squarefree.

We point out that this completes the remaining case in part (c) since powers of 2 are not square free. □

(e) Prove *Korselt's criterion*: An composite number $n$ is a Carmichael number if and only if it is square free and for all prime divisors $p$ of $n$, we have $p - 1|n - 1$.

*Proof.* If $n$ is squarefree and for all prime divisors $p$ of $n$ we have $p - 1|n - 1$, then we know that $n$ is a Carmichael number by Lemma 1. Conversely, suppose $n$ is a Carmichael number. Then we know it is squarefree by part (d). Let $p|n$ be any prime factor, and let $g$ be a primitive root modulo $p$. Then $g^n \equiv g \mod n$ implies $g^n \equiv g \mod p$. Since $g$ is a unit mod $p$ this implies that $g^{n-1} \equiv 1 \mod p$. Since the order of $g$ in $\mathbb{F}_p^*$ is $p - 1$, this implies that $p - 1|n - 1$ as desired. □

7. Here we give another characterization of the Legendre symbol from a group theoretic perspective.

(a) Let $G, H, K$ be groups, and let $\varphi : G \to H$ and $\psi : H \to K$ be homomorphisms. Show that the composition $\psi \circ \varphi : G \to K$ is a homomorphism.

*Proof.* Leg $g, g' \in g$. Then:

$$\begin{aligned} \psi \circ \varphi(g *_G g') &= \psi(\varphi(g *_G g')) \\ &= \psi(\varphi(g) *_H \varphi(g')) \\ &= \psi(\varphi(g)) *_K \psi(\varphi(g')) \\ &= (\psi \circ \varphi(g)) *_K (\psi \circ \varphi(g')) \end{aligned}$$

so that $\psi \circ \varphi$ is a homomorphism. □

(b) Show that the set $\{\pm 1\}$ is a group under multiplication.

*Proof.* Closure under multiplication is clear, and the multiplicative unit is certainly 1. Associativity is inherited from $\mathbb{Z}$. The inverse of 1 is itself, and the inverse of $-1$ is $-1$. □

(c) Let $N$ be a positive even integer. Show that the map $\mathbb{Z}/N\mathbb{Z} \to \{\pm 1\}$ given by the rule $x \mapsto (-1)^x$ is a well defined homomorphism (where the group law for $\mathbb{Z}/N\mathbb{Z}$ is addition).

*Proof.* We first show that the map is well defined. Notice that:

$$(-1)^x = \begin{cases} 1 & x \text{ is even} \\ -1 & x \text{ is odd} \end{cases}.$$

If $x \equiv y \mod N$, then $x \equiv y \mod 2$ since $2|N$ (here we use $N$ is even in an important way!). Therefore $(-1)^x = (-1)^y$ so the map is well defined. To see it is a homomorphism we fix $x, y \in \mathbb{Z}/N\mathbb{Z}$ and represent each by integers (the choice doesn't matter since the map is well defined). Then the normal exponentiation rules imply $(-1)^{x+y} = (-1)^x(-1)^y$ so that the map is indeed a homomorphism. □

(d) Let $p$ be an odd prime, and let $g \in \mathbb{F}_p$ be a primitive root. Show that the composition

$$\mathbb{F}_p^* \xrightarrow{\log_g(\cdot)} \mathbb{Z}/(p-1)\mathbb{Z} \xrightarrow{(-1)^x} \{\pm 1\}$$

is equal to the Legendre function $x \mapsto \left(\frac{x}{p}\right)$. Use this together with part (a)-(c) to give another proof that the Legendre symbol is multiplicative.

*Proof.* By Homework 3 Problem 6, $a \in \mathbb{F}_p^*$ is a quadratic residue if and only if $\log_g(a)$ even. But this holds if and only if $(-1)^{\log_g a} = 1$. So $(-1)^{\log_g a}$ is 1 if and only if $\left(\frac{a}{p}\right) = 1$, completing the proof.

By parts (a) and (c) this composition is a homomorphism, i.e., it commutes with multiplication. Since the composition is equal to the Legendre symbol, this implies the Legendre symbol is multiplicative. □

8. On previous assignments we've extesively studied the notion of squares modulo $p$ (i.e., *quadratic residues mod* $p$), and one thing we noticed is that the situation differed depending on whether $p$ was even or odd (i.e., it depended on the residue of $p$ modulo 2). Here we begin our exploration of cube roots modulo $p$, and we will notice that the story depends on the the residue of $p$ modulo 3. First a definition:

**Definition 2.** *Let $p$ be a prime number. An integer $a$ is called a cubic residue mod $p$ if $p \nmid a$ and there exists an integer $c$ satisfying $c^3 \equiv a \mod p$.*

Let's begin by studying the case where $p \equiv 1 \mod 3$. **For parts (a)-(d), assume** $p \equiv 1 \mod 3$.

(a) Let $a, b$ be cubic residues modulo $p$. Show that $ab$ is a cubic residue mod $p$.

*Proof.* Since $\mathbb{F}_p^*$ is closed under multipication, we see that $p \nmid a, b$ implies $p \nmid ab$. Let $c^3 \equiv a \mod p$ and $d^3 \equiv b \mod p$. Then $(cd)^3 = c^3 d^3 \equiv ab \mod p$ so that $ab$ is indeed a cubic residue. □

(b) Give an example to show that if $a$ and $b$ are cubic nonresidues mod $p$, then $ab$ could also be a nonresidue. Explain why this is different from the situation of quadratic residues.

*Proof.* Let $p = 7$, so that $\mathbb{F}_p^* = \{1, 2, 3, 4, 5, 6\}$. Cubing each gives the cubic residues $(\mathbb{F}_p^*)^3 = \{1, 6\}$. In particular, 3 and 4 are not cubic residues, but their product $12 \equiv 5 \mod 7$ is not a cubic residue either.

For the case of quadratic residues, the multiplicativity of the Legendre symbol shows that the product of two quadratic nonresidues is a quadratic residue, but we see this is not the case for cubic residues. □

(c) Let $g$ be a primitive root for $\mathbb{F}_p$. Show that $a$ is a cubic residue modulo $p$ if and only if $\log_g a$ is a multiple of 3.

*Proof.* We consider the discrete log map:

$$\log_g(\cdot) : \mathbb{F}_p^* \to \mathbb{Z}/(p-1)\mathbb{Z}.$$

Notice that $\log_g(x^3) = 3\log_g(x)$, so in particular, cubing in $\mathbb{F}_p^*$ corresponds to multiplying by 3 in $\mathbb{Z}/(p-1)\mathbb{Z}$. We therefore have the following principle, which we label as a Lemma for future reference.

**Lemma 2.** *Let $a \in \mathbb{F}_p^*$ and let $c = \log_g a$. Then the discrete log map gives a bijection between the cube roots of $a$ mod $p$ and solutions to*

$$3x \equiv c \mod p - 1. \tag{1}$$

*Proof.* Let $b^3 \equiv a \mod p$. Then

$$\log_g b^3 \equiv 3\log_g b \equiv \log_g a = c \mod p - 1,$$

giving a solution to Equation 1. Conversely given a $d$ such that $3d \equiv c \mod p-1$, we have:

$$(g^d)^3 \equiv g^{3d} \equiv g^c \equiv a \mod p.$$

□

With this in hand, solving part (c) is easy. In particular, Lemma 2 implies that $a$ is a cubic residue if and only if there is a solution to Equation 1. By Homework 2 Problem 7(a) such a solution exists if and only if $\gcd(3, p-1)$ divides $c = \log_g a$. Since $p \equiv 1 \mod 3$, $p-1$ is divisible by 3, so that $\gcd(3, p-1) = 3$. In particular, we have showed that $a$ is a cubic residue if and only if 3 divides $\log_g a$, as desired. □

(d) Show that if $a$ is a cubic residue modulo $p$, then $a$ has precisely 3 cube roots modulo $p$.

*Proof.* Suppose $a$ is a cubic residue. By Lemma 2, cube roots of $a$ correspond to solutions to Equation 1. Since we know there is at least one, by Homework 2 Problem 7(b), there are precisely $\gcd(3, p-1)$. Since $p \equiv 1 \mod 3$ we have that $\gcd(3, p-1) = 3$, giving the result. □

(e) Part (c) showed that if $p \equiv 1 \mod 3$ then one third of the elements of $\mathbb{F}_p^*$ have cube roots. The case where $p \equiv 2 \mod 3$ is quite different. Suppose $p \equiv 2 \mod 3$. Show that every integer has a cube root modulo $p$. If $p \nmid a$, how many cube roots does $a$ have mod $p$?

*Proof.* We again apply Lemma 2, noticing that $a$ has a cube root if and only if Equation 1 has a solution. Since $p \equiv 2 \mod 3$, we have $\gcd(3, p-1) = 1$, so that 3 is invertible in $\mathbb{Z}/(p-1)\mathbb{Z}$. In particular, Equation 1 always has a *unique* solution. By Lemma 2 we see that $a$ always has a *unique* cube root! □

(f) Like in the case of square roots mod 2, the case of cube roots mod 3 is different still. Show that every integer has *precisely 1* cube root modulo 3.

*Proof.* By Fermat's little theorem, we have $a^3 \equiv a \mod 3$ for any $a$, so that every element has a unique cube root: *itself*! □

(g) In fact, it is a general principle that $p$th roots modulo $p$ are very simple. Prove that if $p$ is prime every integer has precisely one $p$th root modulo $p$. (*Hint*: Fermat's little theorem.)

*Proof.* By Fermat's little theorem, we have $a^p \equiv a \mod p$ for any $a$, so that every element has a unique cube root: *itself*! □