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.) If they both worked, explain why one worked faster.

   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, and in fact, in taking the limit of this ratio one does get 1.

   That being said, the number does seem < 1 at each step. And in fact, this is something that is observed for any fixed limit even as they get very large. THis observation is called Chebyshev's bias, which says that one usually observes slightly more primes congruent to 3 than to 1. This is currently unproven, though it follows from a strong form of the Riemann Hypothesis.

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 Sun-Tzu's 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 Sun-Tzu's 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. □