Math 437/537—Group Work #5

Tuesday, October 15, 2024

1. We define a ***base-b pseudoprime*** *to be a composite number m such that $b^{m-1} \equiv 1 \pmod{m}$.*

(a) *Using the fact that $2^{10} = 3 \cdot 341 + 1$, show that $2^{341-1} \equiv 1 \pmod{341}$. Conclude that 341 is either a prime or a base-2 pseudoprime.*
(b) *Using the fact that $3^{10} = 173 \cdot 341 + 56$, show that 341 is not a base-3 pseudoprime. (Hint: calculate $56 \cdot 56^2 \pmod{341}$.)*
(c) *Why does the calculation in part (b) prove that 341 is composite?*

(a) The given fact tells us that $2^{10} \equiv 1 \pmod{341}$, and so

$$2^{341-1} = (2^{10})^{34} \equiv 1^{34} = 1 \pmod{341}.$$

If 341 is prime, then it's prime; if it's composite, then it satisfies the definition of a base-2 pseudoprime.

(b) We calculate that $56^2 = 3136 = 9 \cdot 341 + 67 \equiv 67 \pmod{341}$, and so $56 \cdot 56^2 \equiv 56 \cdot 67 = 3752 = 11 \cdot 341 + 1 \equiv 1 \pmod{341}$. Therefore, since we are given that $3^{10} \equiv 56 \pmod{341}$,

$$3^{341-1} = (3^{10})^{34} \equiv 56^{34} = (56^3)^{11} \cdot 56 \equiv 1^{11} \cdot 56 \not\equiv 1 \pmod{341},$$

and so 341 is not a base-3 pseudoprime.

(c) If 341 were prime, then since $(3, 341) = 1$, Fermat's little theorem would tell us that $3^{341-1} \equiv 1 \pmod{341}$. Since this is not the case, we conclude that 341 must be composite.

In this way, we see that Fermat's little theorem can be turned into a compositeness proof: if we find a b (not a multiple of m) for which b^{m-1} fails to be congruent to 1 modulo m, then m must be composite. Prime numbers always pass this test, by Fermat's little theorem; a base-b pseudoprime is a composite number that sneaks by this "(Fermat) base-b pseudoprime test" as a false positive.

As it happens, all of the operations involved in the base-b pseudoprime test (modular exponentiation, computing congruences and gcds) are lightning fast on computers, while actually factoring very large numbers is prohibitively slow. This leads to the strange state of affairs that there are lots of large numbers that we have proved composite, using pseudoprime tests, but which we are unable to factor!

2. We define a ***Carmichael number*** *to be a composite number m such that $b^{m-1} \equiv 1 \pmod{m}$ for every integer b satisfying $(b, m) = 1$. In other words, a Carmichael number is a base-b pseudoprime for every reduced residue b modulo m.*

(a) *Using the fact that $561 = 3 \cdot 11 \cdot 17$, prove that 561 is a Carmichael number.*
(b) *Suppose that k is an integer such that $6k+1$, $12k+1$, and $18k+1$ are all prime. Prove that $(6k + 1)(12k + 1)(18k + 1)$ is a Carmichael number. Deduce that 1729 is a Carmichael number.*

(a) We need to prove that for every $(b, 561) = 1$, we have $b^{560} \equiv 1 \pmod{561}$. By the Chinese remainder theorem, since $3, 11, 17$ are pairwise coprime, this congruence is equivalent to the trio of congruences

$$\begin{aligned}
b^{560} &\equiv 1 \text{ (mod 3)}\\
b^{560} &\equiv 1 \text{ (mod 11)}\\
b^{560} &\equiv 1 \text{ (mod 17)}.
\end{aligned}$$

Note also that b is coprime to 561 if and only if it is coprime to each of $3, 11, 17$. Therefore Fermat's little theorem tells us that

$$\begin{aligned}
b^{2} &\equiv 1 \text{ (mod 3)}\\
b^{10} &\equiv 1 \text{ (mod 11)}\\
b^{16} &\equiv 1 \text{ (mod 17)},
\end{aligned}$$

and therefore

$$\begin{aligned}
b^{560} &= (b^2)^{280} \equiv 1^{280} \equiv 1 \text{ (mod 3)}\\
b^{560} &= (b^{10})^{56} \equiv 1^{56} \equiv 1 \text{ (mod 11)}\\
b^{560} &= (b^{16})^{35} \equiv 1^{35} \equiv 1 \text{ (mod 17)}
\end{aligned}$$

as needed.

(b) Let $m = (6k+1)(12k+1)(18k+1)$. Just as in part (a), we need to show that if $(b, m) = 1$ then $b^{m-1} \equiv 1 \pmod{m}$; by the Chinese remainder theorem, since the three primes $6k+1, 12k+1, 18k+1$ are pairwise coprime, it suffices to show

$$\begin{aligned}
b^{m-1} &\equiv 1 \text{ (mod } 6k+1)\\
b^{m-1} &\equiv 1 \text{ (mod } 12k+1)\\
b^{m-1} &\equiv 1 \text{ (mod } 18k+1).
\end{aligned}\tag{1}$$

Again, $(b, m) = 1$ is equivalent to $(b, 6k+1) = (b, 12k+1) = (b, 18k+1) = 1$, and so Fermat's little theorem tells us that

$$\begin{aligned}
b^{6k} &\equiv 1 \text{ (mod } 6k+1)\\
b^{12k} &\equiv 1 \text{ (mod } 12k+1)\\
b^{18k} &\equiv 1 \text{ (mod } 18k+1).
\end{aligned}\tag{2}$$

As in part (a), to show that the congruences (2) imply the congrences (1), it suffices to show that each of $6k$, $12k$, and $18k$ divides $m = 1$.

Method 1: Multiply out $m-1 = (6k+1)(12k+1)(18k+1) - 1 = 1296k^3 + 396k^2 + 36k = 36k(36k^2 + 11k + 1)$ and note that each of $6k$, $12k$, and $18k$ divides $36k$.

Method 2: Simplify the polynomial multiplication by using $6k$, $12k$, and $18k$ as moduli. For example,

$$(6k+1)(12k+1)(18k+1) - 1 \equiv (6k+1)(-6k+1)(1) = (-36k^2+1) \equiv 1 \text{ (mod } 18k).$$

Since setting $k = 1$ results in the three primes $7, 13, 19$, we conclude that $7 \cdot 13 \cdot 19 = 1729$ is a Carmichael number.

[Side note: the next three Carmichael numbers of this form come from $k = 6, 35, 45$. It is conjectured that there are infinitely many integers k such that $6k+1$, $12k+1$, and $18k+1$ are all prime, but this is still an open problem, similar to but probably harder than the twin primes conjecture.]

The first four Carmichael numbers are 561, 1105, 1729, and 2465. In 1994, Alford, Granville, and Pomerance showed that *there are infinitely many Carmichael numbers*, in the paper of the same name. The existence of Carmichael numbers means that the base-b pseudoprime tests from problem #1 will never be perfect: some composite numbers sneak by all of them.

The method you used in problem #2 is encapsulated in "Korselt's criterion" for a number to be a Carmichael number, if you want to read more about that.

3. *This problem provides another way to show that a number is composite without factoring it.*

(a) *Let m be an odd number and b an integer relatively prime to m. Write $m-1=2^v n$ where n is odd. Consider the sequence*

$$b^n \pmod{m}, \quad b^{2n} \pmod{m}, \quad \dots, \quad b^{2^{v-1}n} \pmod{m}, \quad b^{2^v n} = b^{m-1} \pmod{m}.$$

Suppose that for some $1 \le k \le v$, we have $b^{2^{k-1}n} \not\equiv \pm1 \pmod{m}$ and $b^{2^k n} \equiv 1 \pmod{m}$. Show that m is composite.

(b) *Show that $m = 1729$ is composite by computing the above sequence with $b = 2$. You may use the fact that $2^{27} \equiv 645 \pmod{1729}$.*

(a) We note that $(b^{2^{k-1}n})^2 = b^{2^k n} \equiv 1 \pmod{m}$; therefore $b^{2^{k-1}n}$ is a solution of the congruence $x^2 \equiv 1 \pmod{m}$. If m were prime, then Lemma 2.10 would tell us that the only solutions of $x^2 \equiv 1 \pmod{m}$ are $x \equiv \pm1 \pmod{m}$; but we are given that $b^{2^{k-1}n} \not\equiv \pm1 \pmod{m}$, and so m cannot be prime.

(b) We write $1729 - 1 = 2^6 \cdot 27$, and we calculate

$$\begin{aligned} 2^{54} &= (2^{27})^2 \equiv 645^2 = 416025 \equiv 1065 \not\equiv \pm1 \pmod{1729} \\ 2^{108} &= (2^{54})^2 \equiv 1065^2 = 1134225 \equiv 1 \pmod{1729}. \end{aligned}$$

(Note how the repeated squaring method means that we never have to deal with integers larger than 1729^2.) Thus $m = 1729$ satisfies the assumptions of part (a) with $b = 2$, $n = 27$, and $k = 2$ and is therefore composite.

The base-b pseudoprime test from problem #1 examines just the last number $b^{m-1} \pmod{m}$ in the sequence written in #3(a). Combining that test with the test given in #3(a) yields the "strong Fermat pseudoprime test", which (as we saw) unmasks more composite numbers than the Fermat pseudoprime test alone. Furthermore, the sequence is extremely easy to calculate, by first calculating $b^n \pmod{m}$ and then squaring the result successively v times.

Finally, it can be shown that a composite number m can sneak by this "strong base-b pseudoprime test" for at most $\frac{m}{4}$ residue classes b—there are no "strong Carmichael numbers".