Homework #5

MATH 311 — Intro to Number Theory
due in class on Tuesday, Nov 15

Please print your name:

These problems are not suited to be done last minute!
Also, if you start early, you can consult with me if you should get stuck.

Problem 1.

(a) Evaluate $\phi(2016)$.

(b) Evaluate $\phi(10^n)$.

(c) Use Euler's theorem to compute $2^{666} \pmod{77}$.

Solution.

(a) $\phi(2016) = \phi(2^5 \cdot 3^2 \cdot 7) = 2016\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{7}\right) = 576$

(b) $\phi(10^n) = \phi(2^n \cdot 5^n) = 10^n\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = \frac{2}{5} \cdot 10^n$

(c) Since $\gcd(2, 77) = 1$ and $\phi(77) = 77\left(1 - \frac{1}{7}\right)\left(1 - \frac{1}{11}\right) = 60$, Euler's theorem shows that $2^{60} \equiv 1 \pmod{77}$. Therefore, $2^{666} \equiv 2^6 = 64 \pmod{77}$. □

Problem 2. For any integer a, show that a and a^{4n+1} have the same last (decimal) digit.

Solution. In other words, we need to show that $a^{4n+1} \equiv a \pmod{10}$. By the Chinese remainder theorem, this is the same as showing that $a^{4n+1} \equiv a \pmod{2}$ and $a^{4n+1} \equiv a \pmod{5}$ for all integers a.

$a^{4n+1} \equiv a \pmod{2}$ is true, because it is obviously true for $a \equiv 0 \pmod{2}$ and $a \equiv 1 \pmod{2}$.

By Fermat's little theorem, $a^4 \equiv 1 \pmod{5}$ provided that $\gcd(a, 5) = 1$. In that case, $a^{4n+1} = (a^4)^n \cdot a \equiv a \pmod{5}$. On the other hand, $\gcd(a, 5) > 1$ if and only if $a \equiv 0 \pmod{5}$, in which case we also have $a^{4n+1} \equiv a \pmod{5}$ [because both sides are congruent to 0]. Taken together, $a^{4n+1} \equiv a \pmod{5}$ for all integers a.

Consequently, the Chinese remainder theorem shows that $a^{4n+1} \equiv a \pmod{10}$ for all integers a.

Comment. Note that $\phi(10) = 10\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 4$. Hence, by Euler's theorem $a^4 \equiv 1 \pmod{10}$ if $\gcd(a, 10) = 1$. This immediately implies that $a^{4n+1} = (a^4)^n \cdot a \equiv a \pmod{10}$ for all integers a such that $\gcd(a, 10) = 1$. But we still need to give some argument covering the case that $2|a$ or $5|a$. □

Problem 3. Use Euler's theorem to show that $51|(10^{32n+9} - 7)$ for any integer $n \geqslant 0$.

Solution. In other words, we need to show that $10^{32n+9} \equiv 7 \pmod{51}$.

Since $\phi(51) = \phi(3 \cdot 17) = 51\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{17}\right) = 32$ and $\gcd(10, 51) = 1$, we have $10^{32} \equiv 1 \pmod{51}$ by Euler's theorem.

Consequently, $10^{32n+9} \equiv (10^{32})^n \cdot 10^9 \equiv 10^9 \pmod{51}$. Finally, we compute that, modulo 51, $10^2 \equiv -2$, $10^4 \equiv 4$, $10^8 \equiv 16$, so that $10^9 \equiv 10^8 \cdot 10 \equiv 160 \equiv 7 \pmod{51}$. Taken together, $10^{32n+9} \equiv 10^9 \equiv 7 \pmod{51}$. □

Problem 4.

(a) Show that 25 is a pseudoprime to base 7.

Armin Straub
straub@southalabama.edu

(b) Show that $561 = 3 \cdot 11 \cdot 17$ is an absolute pseudoprime.

Solution.

(a) We need to verify that $7^{25} \equiv 7 \pmod{25}$. Note that $25 = (11001)_2 = 16 + 8 + 1$.

$7^2 \equiv -1$, $7^4 \equiv (-1)^2 = 1$, $7^8 \equiv 1 \pmod{25}$, $7^{16} \equiv 1 \pmod{25}$. Hence, $7^{25} \equiv 7^{16} \cdot 7^8 \cdot 7 \equiv 1 \cdot 1 \cdot 7 \equiv 7 \pmod{25}$.

(b) Let a be any integer. We need to show that $a^{561} \equiv a \pmod{561}$ for all integers a.

By the Chinese remainder theorem, this is the same as showing that $a^{561} \equiv a \pmod{3}$, $a^{561} \equiv a \pmod{11}$ and $a^{561} \equiv a \pmod{17}$ for all integers a.

By Fermat's little theorem, $a^{16} \equiv 1$ (mod 17) provided that $\gcd(a, 17) = 1$. In that case, $a^{561} = (a^{16})^{35} \cdot a \equiv a$ (mod 17). On the other hand, $\gcd(a, 17) > 1$ if and only if $a \equiv 0$ (mod 17), in which case we also have $a^{561} \equiv a \pmod{17}$ [because both sides are congruent to 0]. Taken together, $a^{561} \equiv a \pmod{17}$ for all integers a.

Note that the thing that made this argument work was that 17 is a prime p and that $(p-1)|(561-1)$. The same is true for $p = 11$ (because $10|560$) and $p = 3$ (because $2|560$) so that $a^{561} \equiv a \pmod{3}$ and $a^{561} \equiv a \pmod{11}$ for all integers a.

Consequently, the Chinese remainder theorem shows that $a^{561} \equiv a \pmod{561}$ for all integers a. □

Armin Straub
straub@southalabama.edu