Midterm #2

MATH 311 — Intro to Number Theory
Tuesday, Nov 13

Please print your name:

No notes or tools of any kind are permitted. There are 28 points in total. You need to show work to receive full credit.

Good luck!

Problem 1. (4 points) Using the Chinese remainder theorem, determine all solutions to $x^2 \equiv 1 \pmod{77}$.

Solution. By the Chinese remainder theorem (CRT):

$$\begin{aligned} & x^2 \equiv 1 \pmod{77} \\ \iff\ & x^2 \equiv 1 \pmod{7} \text{ and } x^2 \equiv 1 \pmod{11} \\ \iff\ & x \equiv \pm 1 \pmod{7} \text{ and } x \equiv \pm 1 \pmod{11} \end{aligned}$$

The two obvious solutions modulo 77 are ± 1. To get one of the two additional solutions, we solve $x \equiv 1 \pmod{7}$, $x \equiv -1 \pmod{11}$. [Then the other additional solution is the negative of that.]

$$x \equiv 1 \cdot 11 \cdot \underbrace{11^{-1}_{\bmod 7}}_{2} - 1 \cdot 7 \cdot \underbrace{7^{-1}_{\bmod 11}}_{-3} \equiv 22 + 21 \equiv 43 \equiv -34 \pmod{77}$$

Hence, the solutions are $x \equiv \pm 1 \pmod{77}$ and $x \equiv \pm 34 \pmod{77}$. □

Problem 2. (2 points) Suppose that $x^a \equiv 1 \pmod{n}$ and $x^b \equiv 1 \pmod{n}$. Show that $x^{\gcd(a,b)} \equiv 1 \pmod{n}$.

Solution. By Bezout's identity, we find integers r, s such that $ra + sb = \gcd(a, b)$. Hence,

$$x^{\gcd(a,b)} = x^{ra+sb} = (x^a)^r \cdot (x^b)^s \equiv 1^r \cdot 1^s \equiv 1 \pmod{n}.$$ □

Armin Straub
straub@southalabama.edu

Problem 3. (3 points) What is the last (decimal) digit of 7^{123456}?

Solution. We need to determine $7^{123456} \pmod{10}$. Since $\gcd(7,10)=1$ and $\phi(10)=\phi(2)\phi(5)=4$ and $123456 \equiv 56 \equiv 0 \pmod{4}$, we have $7^{123456} \equiv 7^0 \equiv 1 \pmod{10}$. This means that the last (decimal) digit of 7^{123456} is 1. □

Problem 4. (4 points) Obviously, 15 is not a prime. Is 7 a Fermat liar modulo 15? Is 4 a Fermat liar modulo 15?

Solution. 7 is a Fermat liar modulo 15 if and only if $7^{14} \equiv 1 \pmod{15}$.

$7^2 \equiv 4 \pmod{15}$, $7^4 \equiv 1 \pmod{15}$, $7^8 \equiv 1 \pmod{15}$. Hence, $7^{14} \equiv 7^8 \cdot 7^4 \cdot 7^2 \equiv 1 \cdot 1 \cdot 4 \equiv 4 \pmod{15}$.

Since $7^{14} \not\equiv 1 \pmod{15}$, 7 is not a Fermat liar modulo 15.

On the other hand, $4^2 \equiv 1 \pmod{15}$, so that $4^{14} \equiv 1 \pmod{15}$. Hence, 4 a Fermat liar modulo 15. □

Problem 5. (3 points) Briefly outline the Fermat primality test.

Solution. Fermat primality test:

Input: number n and parameter k indicating the number of tests to run
Output: "not prime" or "possibly prime"
Algorithm:

Repeat k times:
  Pick a random number a from $\{2, 3, ..., n-2\}$.
  If $a^{n-1} \not\equiv 1 \pmod{n}$, then stop and output "not prime".
Output "possibly prime". □

Armin Straub
straub@southalabama.edu

Problem 6. (12 points)

(a) Among the numbers $1, 2, ..., 54$, how many are coprime to 54? $\boxed{}$.

(b) If $n = p^2 q$, for distinct primes p, q, then $\phi(n) = \boxed{}$.

(c) How many solutions does the congruence $x^2 \equiv 4 \pmod{105}$ have? $\boxed{}$

(d) How many solutions does the congruence $x^2 \equiv 4 \pmod{210}$ have? $\boxed{}$

(e) How many solutions does the congruence $x^2 \equiv 4 \pmod{3135}$ have? $\boxed{}$ $(3135 = 3 \cdot 5 \cdot 11 \cdot 19)$

(f) $x = 30$ is a solution to $\begin{matrix} x \equiv 30 \pmod{100} \\ x \equiv 8 \pmod{11} \end{matrix}$. Another positive solution is $\boxed{}$.

(g) The multiplicative order of $3 \pmod{11}$ is $\boxed{}$.

Armin Straub
straub@southalabama.edu

(h) The multiplicative order of $x \pmod{88}$ divides $\boxed{}$.

(i) The primitive roots modulo 7 are $\boxed{}$.

(j) If $x \pmod{n}$ has multiplicative order k, then x^{2018} has multiplicative order $\boxed{}$.

(k) What is the number of invertible residues modulo 29? $\boxed{}$

(l) What is the number of primitive roots modulo the prime 89? $\boxed{}$

Solution.

(a) $\phi(54) = \phi(2)\phi(27) = 27 - 9 = 18$

(b) If $n = p^2 q$, for distinct primes p, q, then $\phi(n) = \phi(p^2)\phi(q) = (p^2 - p)(q - 1)$.

(c) By the CRT, since $105 = 3 \cdot 5 \cdot 7$, the congruence has $2 \cdot 2 \cdot 2 = 8$ solutions.

(d) By the CRT, since $210 = 2 \cdot 3 \cdot 5 \cdot 7$, the congruence has $1 \cdot 2 \cdot 2 \cdot 2 = 8$ solutions. (Note that $x^2 \equiv 4 \pmod{2}$ only has one solution; namely, $x \equiv 0$.)

(e) By the CRT, since $3135 = 3 \cdot 5 \cdot 11 \cdot 19$, the congruence has $2 \cdot 2 \cdot 2 \cdot 2 = 16$ solutions.

(f) The next largest positive solution is $30 + 100 \cdot 11 = 1130$.

(g) The multiplicative order of $3 \pmod{11}$ is 5.

(h) The multiplicative order of x modulo 88 divides $\phi(88) = \phi(8)\phi(11) = (8 - 4) \cdot 10 = 40$.

(i) The primitive roots modulo 7 are $3, 5$.

(j) If $x \pmod{n}$ has multiplicative order k, then x^{2018} has multiplicative order $\frac{k}{\gcd(k, 2018)}$.

(k) $\phi(29) = 28$

(l) $\phi(\phi(89)) = \phi(88) = 40$ □

(extra scratch paper)