Midterm #2

MATH 311 — Intro to Number Theory
Tuesday, Nov 12

Please print your name:

No notes or tools of any kind are permitted. There are 37 points in total. You need to show work to receive full credit.

Good luck!

Problem 1. (4 points) Determine $91^{88} \pmod{88}$.

Solution. Clearly, $91^{88} \equiv 3^{88} \pmod{88}$. Since $\gcd(3, 88) = 1$ as well as $\phi(88) = \phi(2^3)\phi(11) = (2^3 - 2^2) \cdot 10 = 40$ and $88 \equiv 8 \pmod{40}$, we have $91^{88} \equiv 3^8 \pmod{88}$.

Binary exponentiation: $3^2 = 9$, $3^4 = 81 \equiv -7$, $3^8 \equiv 49 \pmod{88}$.

Hence, $91^{88} \equiv 49 \pmod{88}$. □

Problem 2. (4 points) Use Euler's criterion to answer the following questions. p is an odd prime and $x \not\equiv 0 \pmod{p}$.

(a) By Euler's criterion, $x \pmod{p}$ is a quadratic residue if and only if [ ].

(b) $7 \pmod{17}$ ☐ is a quadratic residue ☐ is not a quadratic residue because [ ].

(c) $7 \pmod{19}$ ☐ is a quadratic residue ☐ is not a quadratic residue because [ ].

Solution.

(a) $x \pmod{p}$ is a quadratic residue if and only if $x^{(p-1)/2} \equiv 1 \pmod{p}$.

(b) We compute $7^8 \pmod{17}$ using binary exponentiation: $7^2 \equiv -2$, $7^4 \equiv 4$, $7^8 \equiv 16 \equiv -1 \pmod{17}$. In particular, $7^8 \equiv -1 \pmod{17}$. Hence, by Euler's criterion, 7 is not a quadratic residue modulo 17.

(c) We compute $7^9 \pmod{19}$ using binary exponentiation: $7^2 \equiv -8$, $7^4 \equiv 64 \equiv 7$, $7^8 \equiv -8 \pmod{19}$ so that $7^9 \equiv 7 \cdot (-8) \equiv 1 \pmod{19}$. Hence, by Euler's criterion, 7 is a quadratic residue modulo 19. □

Armin Straub
straub@southalabama.edu

Problem 3. **(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". □

Problem 4. **(5 points)** Find the smallest positive integer x simultaneously solving the three congruences:

$$\begin{aligned} 2x &\equiv 1 \pmod{3} \\ 3x &\equiv 2 \pmod{7} \\ 7x &\equiv 1 \pmod{10} \end{aligned}$$

Solution. Equivalently, we need to solve $x \equiv -1 \pmod{3}$, $x \equiv 3 \pmod{7}$, $x \equiv 3 \pmod{10}$.

Since $3 \cdot 7 \cdot 10 = 210$, by the Chinese remainder theorem, the general solution is

$$x \equiv -1 \cdot 70 \cdot \underbrace{70^{-1}_{\text{mod } 3}}_{1} + 3 \cdot 30 \cdot \underbrace{30^{-1}_{\text{mod } 7}}_{4} + 3 \cdot 21 \cdot \underbrace{21^{-1}_{\text{mod } 10}}_{1} \equiv -70 + 360 + 63 \equiv 143 \pmod{210}.$$

The smallest positive integer solution therefore is $x = 143$. □

Armin Straub
straub@southalabama.edu

Problem 5. (4 points)

(a) Suppose N is composite. x is a Fermat liar modulo N if and only if $\boxed{}$.

(b) $7 \pmod{15}$ ☐ is a Fermat liar ☐ is not a Fermat liar because $\boxed{}$.

(c) $4 \pmod{15}$ ☐ is a Fermat liar ☐ is not a Fermat liar because $\boxed{}$.

Solution.

(a) x is a Fermat liar modulo N if and only if $x^{N-1} \equiv 1 \pmod{N}$.

(b) 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.

(c) 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 6. (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,

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

□

Problem 7. (3 points)

(a) What is the number of invertible residues modulo 55? $\boxed{}$

(b) What is the number of invertible quadratic residues modulo 55? $\boxed{}$

(c) What is the number of invertible quadratic residues modulo 165? $\boxed{}$

Solution.

(a) $\phi(55) = \phi(5)\phi(11) = 40$

(b) Since $55 = 5 \cdot 11$ is a product of two distinct odd primes, there are $\frac{1}{4}\phi(55) = \frac{40}{4} = 10$ invertible quadratic residues modulo 55.

(c) Since $165 = 3 \cdot 5 \cdot 11$ is a product of three distinct odd primes, there are $\frac{1}{8}\phi(165) = \frac{2 \cdot 4 \cdot 10}{8} = 10$ invertible quadratic residues modulo 165. □

Problem 8. (12 points)

(a) List all quadratic residues modulo 11: ☐

(b) You wonder whether $23,377$ is a prime. A quick computation shows that $2^{23376} \equiv 1 \pmod{23,377}$.

What do you conclude? ☐

(c) How many solutions does the congruence $x^2 \equiv 4 \pmod{33}$ have? ☐

(d) How many solutions does the congruence $x^2 \equiv 9 \pmod{33}$ have? ☐

(e) How many solutions does the congruence $x^2 \equiv 1 \pmod{165}$ have? ☐ $(165 = 3 \cdot 5 \cdot 11)$

(f) $x = 32$ is a solution to $\begin{matrix} x \equiv 1 \pmod{31} \\ x \equiv 2 \pmod{10} \end{matrix}$. The next largest positive solution is ☐.

(g) The multiplicative order of $x \pmod{20}$ divides ☐.

(h) The multiplicative order of $3 \pmod{20}$ is ☐.

Armin Straub
straub@southalabama.edu

(i) If $x \pmod{n}$ has multiplicative order 100, then x^c has multiplicative order $\boxed{}$.

(j) What is the number of primitive roots modulo the prime 29? $\boxed{}$

(k) Wilson's theorem states that, for all primes p, $\boxed{}$.

(l) Suppose that x is a primitive root modulo 19. List all exponents c (between 0 and 18) such that x^c is a primitive root modulo 19. $\boxed{}$

Solution.

(a) $0^2 = 0,\ (\pm 1)^2 = 1,\ (\pm 2)^2 = 4,\ (\pm 3)^2 = 9,\ (\pm 4)^2 \equiv 5,\ (\pm 5)^2 \equiv 3 \pmod{11}$

In summary, the quadratic residues are $0, 1, 3, 4, 5, 9$.

(b) We still don't know whether $23,377$ is a prime or not. There is two possibilities: either $23,377$ is a prime, or $23,377$ is a pseudoprime to base 2 (equivalently, 2 is a Fermat liar modulo $23,377$).

[Actually, $23,377 = 97 \cdot 241$ is not a prime.]

(c) By the CRT, since $33 = 3 \cdot 11$, the congruence has $2 \cdot 2 = 4$ solutions.

(d) By the CRT, since $33 = 3 \cdot 11$, the congruence has $1 \cdot 2 = 2$ solutions. (Note that $x^2 \equiv 9 \pmod{3}$ only has one solution; namely, $x \equiv 0$.)

(e) By the CRT, since $165 = 3 \cdot 5 \cdot 11$, the congruence has $2 \cdot 2 \cdot 2 = 8$ solutions.

(f) The next largest positive solution is $32 + 10 \cdot 31 = 342$.

(g) The multiplicative order of x modulo 20 divides $\phi(20) = \phi(2^2)\phi(5) = 2 \cdot 4 = 8$.

(h) The multiplicative order of $3 \pmod{20}$ is 4.

(i) If $x \pmod{n}$ has multiplicative order 100, then x^c has multiplicative order $\frac{100}{\gcd(c, 100)}$.

(j) $\phi(\phi(29)) = \phi(28) = \phi(4)\phi(7) = 2 \cdot 6 = 12$

(k) Wilson's theorem states that, for all primes p, $(p-1)! \equiv -1 \pmod{p}$.

(l) The exponents are precisely those coprime to 18: $1, 5, 7, 11, 13, 17$ □

(extra scratch paper)

Armin Straub
straub@southalabama.edu