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 $91^{88} \pmod{88}$.

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 .

(scratch space: show your work for partial credit)

Armin Straub
straub@southalabama.edu

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

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

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

Problem 5. (4 points)

(a) Suppose N is composite. x is a Fermat liar modulo N if and only if [ ].

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

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

(scratch space: show your work for partial credit)

Problem 6. (2 points) Suppose that $x^a \equiv 1 \pmod{n}$ and $x^b \equiv 1 \pmod{n}$. Show that $x^{\gcd(a,b)} \equiv 1 \pmod{n}$.

Problem 7. (3 points)

(a) What is the number of invertible residues modulo 55? [ ]

(b) What is the number of invertible quadratic residues modulo 55? [ ]

(c) What is the number of invertible quadratic residues modulo 165? [ ]

(scratch space)

Armin Straub
straub@southalabama.edu

Problem 8. (12 points)

(a) List all quadratic residues modulo 11: $\boxed{}$

(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? $\boxed{}$

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

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

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

(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 $\boxed{}$.

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

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

(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. $\boxed{}$

(scratch space)

(extra scratch paper)