Midterm #3

MATH 311 — Intro to Number Theory
Thursday, Nov 17

Please print your name:

No notes or tools of any kind are permitted. There are 26 points in total. You need to show work to receive full credit.

Good luck!

Problem 1. (3 points) Obviously, 15 is not a prime. Is 15 a pseudoprime to the base 7?

Solution. 15 a pseudoprime to the base 7 if and only if $7^{15} \equiv 7 \pmod{15}$.

$7^2 \equiv 4 \pmod{15}$, $7^4 \equiv 1 \pmod{15}$, $7^8 \equiv 1 \pmod{15}$. Hence, $7^{15} \equiv 7^8 \cdot 7^4 \cdot 7^2 \cdot 7 \equiv 1 \cdot 1 \cdot 4 \cdot 7 \equiv 13 \pmod{15}$.

Since $7^{15} \not\equiv 7 \pmod{15}$, 15 is not a pseudoprime to the base 7. □

Problem 2. (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 3. (3 points) What is the last (decimal) digit of 3^{14159}?

Solution. We need to determine 3^{14159} (mod 10). Since gcd(3, 10) = 1 and $\phi(10) = 10\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 4$ and $14159 \equiv 59 \equiv 3 \pmod{4}$, we have $3^{14159} \equiv 3^3 \equiv 7 \pmod{10}$. This means that the last (decimal) digit of 3^{14159} is 7. □

Armin Straub
straub@southalabama.edu

Problem 4. (2 points) Carefully state Wilson's theorem.

Solution. If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$. $\square$

Problem 5. (3 points) Express the number $\frac{89}{69}$ as a simple continued fraction.

Solution. The simplest way to obtain the continued fraction for $\frac{89}{69}$ is via the Euclidian algorithm:

$$89 = \boxed{1} \cdot 69 + 20, \quad 69 = \boxed{3} \cdot 20 + 9, \quad 20 = \boxed{2} \cdot 9 + 2, \quad 9 = \boxed{4} \cdot 2 + 1, \quad 2 = \boxed{2} \cdot 1 + 0$$

Hence, $\frac{89}{69} = [1; 3, 2, 4, 2]$. $\square$

Problem 6. (2+2 points)

(a) Determine the convergents C_0, C_1, C_2, C_3 of the infinite continued fraction $[1; 4, 1, 4, 1, 4, 1, 4, \ldots]$.

(b) Which number is represented by the infinite continued fraction $[1; 4, 1, 4, 1, 4, 1, 4, \ldots]$?

Solution.

(a) $C_0 = 1$, $C_1 = 1 + \frac{1}{4} = \frac{5}{4}$, $C_2 = 1 + \frac{1}{4 + \frac{1}{1}} = \frac{6}{5}$, $C_3 = 1 + \frac{1}{4 + \frac{1}{1 + \frac{1}{4}}} = 1 + \frac{1}{4 + \frac{4}{5}} = 1 + \frac{5}{24} = \frac{29}{24}$

(b) Write $x = [1; 4, 1, 4, 1, 4, 1, 4, \ldots]$. Then, $x = 1 + \frac{1}{4 + \frac{1}{1 + \frac{1}{4 + \frac{1}{1 + \ldots}}}} = 1 + \frac{1}{4 + \frac{1}{x}}$.

The equation $x = 1 + \frac{1}{4 + \frac{1}{x}}$ simplifies to $x - 1 = \frac{x}{4x + 1}$. Further (note that, clearly $x \neq -\frac{1}{4}$ so that $4x + 1 \neq 0$) simplifies to $(x-1)(4x+1) = x$ or $4x^2 - 4x - 1 = 0$, which has the solutions $x = \frac{4 \pm \sqrt{16 + 16}}{8} = \frac{1 \pm \sqrt{2}}{2}$.

Since $\frac{1 - \sqrt{2}}{2} < 0$, we conclude that $[1; 4, 1, 4, 1, 4, 1, 4, \ldots] = \frac{1 + \sqrt{2}}{2}$. $\square$

Armin Straub
straub@southalabama.edu

Problem 7. **(1 point)** Among the numbers $1, 2, \ldots, 54$, how many are coprime to 54?

Solution. $\phi(54) = \phi(2 \cdot 3^3) = 54\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 18$ many of the numbers $1, 2, \ldots, 54$ are coprime to 54. □

Problem 8. **(1 point)** List all (nonzero) quadratic residues modulo 7.

Solution. $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 \equiv 2 \pmod{7}$. Hence, the quadratic residues modulo 7 are $1, 2, 4$. □

Problem 9. **(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 10. **(4 points)** Using the Chinese remainder theorem, determine all solutions to $x^2 \equiv 1 \pmod{55}$.

Solution. Note that $55 = 5 \cdot 11$. By the Chinese remainder theorem, x is a solution to $x^2 \equiv 1 \pmod{55}$ if and only if x is a solution to $x^2 \equiv 1 \pmod{5}$ as well as $x^2 \equiv 1 \pmod{11}$.

Since 5 and 11 are primes each of these only has the obvious solutions $x \equiv \pm 1$. Using the Chinese remainder theorem, these combine in $2 \cdot 2 = 4$ different ways to a solution modulo 55.

$$\begin{aligned}
x \equiv 1 \pmod{5}, \quad x \equiv 1 \pmod{11} &\iff x \equiv 1 \pmod{55} \\
x \equiv -1 \pmod{5}, \quad x \equiv -1 \pmod{11} &\iff x \equiv -1 \pmod{55} \\
x \equiv 1 \pmod{5}, \quad x \equiv -1 \pmod{11} &\iff x \equiv 1 \cdot 11 \cdot \underbrace{[(11)^{-1}_{\text{mod } 5}]}_{1} - 1 \cdot 5 \cdot \underbrace{[(5)^{-1}_{\text{mod } 11}]}_{-2} = 11 + 10 \equiv 21 \pmod{55} \\
x \equiv -1 \pmod{5}, \quad x \equiv 1 \pmod{11} &\iff x \equiv -21 \pmod{55}
\end{aligned}$$

In summary, $x^2 \equiv 1 \pmod{55}$ has exactly the 4 solutions $x \equiv \pm 1, \pm 21$ modulo 55. □

(extra scratch paper)