Midterm Exam

Math 110
10 February 2015
Jenny Wilson

Name: _____

Instructions: This exam has 10 questions for a total of 40 points plus 5 bonus points.

You may bring in a basic calculator. No books, notes, cell phones, or advanced calculators are permitted. Scratch paper is available.

Please show your work clearly in the space provided. Solutions may not receive full credit without legible work shown. Partial credit may be given for correct work, even if there is a mistake in the final answer.

You have 75 minutes to complete the exam. If you finish early, consider checking your work for accuracy.

Jenny is available to answer questions around the corner from the classroom.

Question	Points	Score
1	3	
2	5	
3	4	
4	2	
5	2	
6	5	
7	4	
8	10	
9	5	
10	0	
Total:	40	

1. (3 points) Compute the set of all integer solutions (u, v) to the equation

$$102u + 45v = 3.$$

You do not need to formally prove that your answer is correct, but please show your work.

2. (5 points) Alonso and Benita are communicating using RSA. Benita publishes the modulus $n = 3131$ and the encryption exponent $e = 353$. Alonso returns the encrypted message 686. Given the factorization $n = (31)(101)$, decrypt Alonso's message. Show your work.

   You may find the following helpful:

   $686^2 \equiv 946 \pmod{3131}$
   $946^2 \equiv 2581 \pmod{3131}$
   $2581^2 \equiv 1924 \pmod{3131}$
   $1924^2 \equiv 934 \pmod{3131}$
   $934^2 \equiv 1938 \pmod{3131}$
   $1938^2 \equiv 1775 \pmod{3131}$
   $1775^2 \equiv 839 \pmod{3131}$
   $839^2 \equiv 2577 \pmod{3131}$

3. (4 points) Akira wishes to send a message to Bo using the ElGamal public key cryptosystem. Describe the steps in their exchange, and briefly explain why it is hard for the eavesdropper Evita to intercept their message.

4. (2 points) Suppose that x is an integer satisfying $19^x \equiv 2 \pmod{29}$. Given that 19 is a primitive root of 29, is x even or odd?

   No formal justification needed, but please show your work.

5. (2 points) Ahmad and Brianna wish to use the Diffie–Hellman key exchange to establish a secret shared key K. Ahmad publishes the prime $p = 1009$ and the primitive root 51 (mod 1009). Brianna selects the exponent $y = 3$ and publishes $51^3 \equiv 472 \pmod{1009}$. Ahmad selects an exponent x publishes $51^x \equiv 22 \pmod{1009}$. What key K do they establish?

   No formal justification needed, but please show your work.

6. (5 points) Given the factorization $989 = (23)(43)$, find all solutions to the equation

$$x^2 \equiv 6 \pmod{989}.$$

Show your work.

7. (4 points) (a) Given that $\gcd(8647, 111) = 1$, compute the Jacobi symbol $\left(\frac{111}{8647}\right)$. Show your work.

(b) What can you conclude (if anything) about whether the congruence 111 is a square modulo 8647? Justify your answer.

8. (10 points) State whether each of the following assertions is always true by writing "`True`" or "`False`". No justification necessary.

   (a) The congruence class [21] modulo 33 is a zero divisor.

   (b) Let $a, b, d \in \mathbb{Z}$. If $\gcd(a, b) = d$, then $\gcd\left(\frac{a}{d}, b\right) = 1$.

   (c) The equation $15x \equiv 5 \pmod{18}$ has one or more solutions $x \in \mathbb{Z}$.

   (d) If $d, n > 1$ are integers and d divides n, then each congruence class modulo d is the union of $\frac{n}{d}$ congruence classes modulo n.

   (e) There are $(12)(26) = 312$ distinct invertible affine ciphers $f(x) = \alpha x + \beta$, for $\alpha, \beta \in \mathbb{Z}/26\mathbb{Z}$.

   (f) The congruence class $[-1]$ can never be a square modulo a prime p.

   (g) Since $3^{1048} \equiv 1 \pmod{1049}$, we can conclude that 1049 is prime.

   (h) Let p be a positive prime. Then any nonzero congruence class modulo p has either zero or two square roots.

   (i) If $n = pq$ is the product of two primes congruent to 3 (mod 4), and y is a unit and a square modulo n, then finding four distinct solutions to $x^2 \equiv y \pmod{n}$ is computationally equivalent to factoring n.

   (j) A prime number p is a square modulo 41 if and only if 41 is a square modulo p.

9. (5 points) (a) Suppose $n > 0 \in \mathbb{Z}$ and a is a congruence class modulo n. Define the multiplicative order $\mathrm{ord}_n(a)$ of a.

Let $a, s, t, n \in \mathbb{Z}$. Prove that

$$a^s \equiv a^t \pmod{n} \qquad \text{if and only if} \qquad s \equiv t \pmod{\mathrm{ord}_n(a)}.$$

(Blank page for extra work)

10. (5 points (bonus)) Let $m, n, d, a, b \in \mathbb{Z}$ and suppose that $\gcd(m, n) = d$. Prove that if $a \equiv b \pmod{d}$, then there exist solutions to the simultaneous system of equations

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}.$$

(Blank page for extra work)