Final Exam

Math 110
19 March 2015
Jenny Wilson

Name: ____

Instructions: This exam has 17 questions for a total of 70 points and 4 bonus points.

You may bring in a basic calculator. You may bring in a one double-sided sheet of notes on standard (8.5" × 11") letter paper. The notes may be handwritten or typed, but you must prepare them yourself.

Otherwise, no books, notes, electronic aids, cell phones, advanced calculators, or other outside material is permitted. Scratch paper is available.

Please hand in your sheet of notes with the exam. You can pick it up again from Jenny once the exams are graded.

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 3 hours 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	4	
2	4	
3	4	
4	3	
5	2	
6	5	
7	3	
8	4	
9	3	
10	9	
11	10	
12	3	
13	5	
14	2	
15	5	
16	4	
17	0	
Total:	70	

1. (4 points) Find all solutions to $x^2 + 28x + 31 \equiv 0 \pmod{35}$, using a method other than simply testing all 35 congruence classes modulo 35. **Show your work.**

2. (a) (2 points) Andrei and Bruno are using RSA with modulus $n = pq = 9991$. Naively, Bruno chose values of p and q with a very small difference. Use this information to factor n. **Show your work.**

(b) (2 points) Amélie and Becca are using RSA with modulus $n = pq = 5671$. The eavesdropper Erin discovers that $639^2 \equiv 9 \pmod{n}$. Show how Erin uses this information to factor n.

3. (4 points) Use the Miller–Rabin test with a base b of your choice to investigate whether $n = 221$ is prime. What can you conclude?

4. (3 points) The prime $p = 83$ has primitive root 5. Solve $5^x \equiv 42 \pmod{83}$, given that:

$$\begin{aligned} 5^6 &\equiv 21 \pmod{83} \\ 5^8 &\equiv 27 \pmod{83} \\ 5^{21} &\equiv 24 \pmod{83} \end{aligned}$$

Use a method other than guess-and-check. **Show your work.**

5. (2 points) The prime $p = 47$ has primitive root 10. Solve $10^x \equiv 30 \pmod{47}$.
Show your work.

$$\begin{aligned}
10^{-1} &\equiv 33 \pmod{47} \\
10^{0} &\equiv 1 \pmod{47} \\
10^{1} &\equiv 10 \pmod{47} \\
10^{2} &\equiv 6 \pmod{47} \\
10^{3} &\equiv 13 \pmod{47} \\
10^{4} &\equiv 36 \pmod{47} \\
10^{5} &\equiv 31 \pmod{47} \\
10^{6} &\equiv 28 \pmod{47}
\end{aligned}$$

$$\begin{aligned}
(30) \cdot (33^{0}) &\equiv 30 \pmod{47} \\
(30) \cdot (33^{7}) &\equiv 32 \pmod{47} \\
(30) \cdot (33^{14}) &\equiv 31 \pmod{47} \\
(30) \cdot (33^{21}) &\equiv 8 \pmod{47} \\
(30) \cdot (33^{28}) &\equiv 43 \pmod{47} \\
(30) \cdot (33^{35}) &\equiv 2 \pmod{47} \\
(30) \cdot (33^{42}) &\equiv 46 \pmod{47}
\end{aligned}$$

6. Let $\mathcal{A}^n$ be a set of length-n words in some alphabet $\mathcal{A}$. Suppose that two words u and v are Hamming distance $d(u,v) \geq (2t+1)$ apart for some $t \in \mathbb{Z}$.

   (a) (1 point) Define the *Hamming sphere* of radius t around a word w.

   (b) (2 points) Prove that the Hamming spheres of radius t around u and v are disjoint, that is, no word is contained in both spheres. You can assume without proof that Hamming distance satisfies the triangle inequality.

   (c) (2 points) Conclude that a code with minimal distance $d \geq 2t+1$ can correct t errors (using nearest-neighbour decoding).

7. (3 points) Prove that a binary (7, 17, 3) code cannot exist. Give a justification for any "bounds on codes" that you use.

8. Let C be the $[5, 2]$ linear binary code associated to the generator matrix

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

(a) (1 point) List all codewords in C, and state the minimal distance.

(b) (1 point) Write down a parity check matrix for the code C, and compute the syndrome of $v = (1, 0, 0, 1, 1)$.

(c) (1 point) Write down all vectors in the coset $v + C$, and identify a coset leader.

(d) (1 point) Find the nearest codeword (in Hamming distance) to v.

9. (3 points) Let $P(x)$ be the irreducible polynomial $P(x) = x^3 + 2x + 1$ with coefficients in $\mathbb{Z}/3\mathbb{Z}$. Find a multiplicative inverse for $(x + 1)$ modulo $P(x)$. **Show your work.**

10. (9 points) State whether each of the following assertions is always true by writing "True" or "False". **No justification necessary.**

(a) If ϕ is Euler's totient function, then $\phi(nm) = \phi(n)\phi(m)$ for any integers n and m.

(b) The equation $x^{28} \equiv 1 \pmod{29}$ has exactly 28 solutions in $\mathbb{Z}/29\mathbb{Z}$.

(c) The Jacobi symbol $\left(\dfrac{122}{1235}\right) = 1$.

(d) Suppose $\phi(n)$ is even and $\mathbb{Z}/n\mathbb{Z}$ has a primitive root. Then exactly half the units in $\mathbb{Z}/n\mathbb{Z}$ are squares.

(e) For $b \in \mathbb{Z}$ not a multiple of 103, exactly one of b and $-b$ is a square modulo the prime 103.

(f) If n has a prime factor p such that $p - 1 = 2^3 3^2$, then n can be successfully factored using the $(p-1)$ algorithm with bound $B = 5$.

(g) Running the Miller-Rabin test with base b may allow us to find a nontrivial factor of a composite integer n, but only if n is a Fermat pseudoprime to the base b.

(h) If a linear code C has minimal distance d, then there is a codeword in C with Hamming weight d.

(i) The subset of rational numbers $\left\{ \dfrac{b}{2^r} \;\middle|\; b \in \mathbb{Z},\ 0 < r \in \mathbb{Z} \right\}$ is a field.

11. (10 points) Give examples of each of the following, or briefly state why an example cannot exist.

    (a) An integer n so that $\mathbb{Z}/n\mathbb{Z}$ contains exactly 8 units.

    (b) An integer $n > 1$ that cannot be a primitive root for any prime $p > 2$.

    (c) A prime $p > 7$ such that 7 is a square modulo p, but p is not a square modulo 7.

    (d) A positive prime p such that $10^2 \equiv 21^2 \pmod{p}$.

    (e) A ternary linear code with $M = 6$ codewords.

    (f) A $[3, 2]$ binary linear code.

    (g) A $(5, 3, 5)$ code.

    (h) A code with code rate $2/3$.

    (i) A finite field of characteristic 6.

    (j) An elliptic curve E over $\mathbb{Z}/5\mathbb{Z}$ along with two of the points on the curve.

12. (3 points) Let $\mathbb{F}$ be a field. Let 1 denote the multiplicative identity, and (-1) denote its additive inverse. Use the field axioms to prove that $(-1) \cdot (-1) = 1$.

Definition. A *field* is a set $\mathbb{F}$ with two binary operations on $\mathbb{F}$ called addition, denoted $+$, and multiplication, denoted $\cdot$, satisfying the following *field axioms*:

FA0 **(Closure under Addition)** For all $x, y \in \mathbb{F}$, the sum $x + y$ is contained in $\mathbb{F}$

FA0 **(Closure under Multiplication)** For all $x, y \in \mathbb{F}$, the product $x \cdot y$ is contained in $\mathbb{F}$.

FA1 **(Commutativity of Addition)** For all $x, y \in \mathbb{F}$, $x + y = y + x$.

FA2 **(Associativity of Addition)** For all $x, y, x \in \mathbb{F}$, $(x + y) + z = x + (y + z)$.

FA3 **(Additive Identity)** There exists an element $0 \in \mathbb{F}$ such that $x + 0 = 0 + x = x$ for all $x \in \mathbb{F}$.

FA4 **(Additive Inverses)** For any $x \in \mathbb{F}$, there exists $y \in \mathbb{F}$ such that $x + y = y + x = 0$.

FA5 **(Commutativity of Multiplication)** For all $x, y \in \mathbb{F}$, $x \cdot y = y \cdot x$.

FA6 **(Associativity of Multiplication)** For all $x, y, z \in \mathbb{F}$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

FA7 **(Multiplicative Identity)** There exists an element $1 \in \mathbb{F}$ such that $x \cdot 1 = 1 \cdot x = x$ for all $x \in \mathbb{F}$.

FA8 **(Multiplicative Inverses)** For any $x \in \mathbb{F}$ such that $x \neq 0$, there exists $y \in \mathbb{F}$ such that $x \cdot y = y \cdot x = 1$.

FA9 **(Distributivity of Multiplication over Addition)** For all $x, y, z \in \mathbb{F}$, $x \cdot (y + z) = x \cdot y + x \cdot z$.

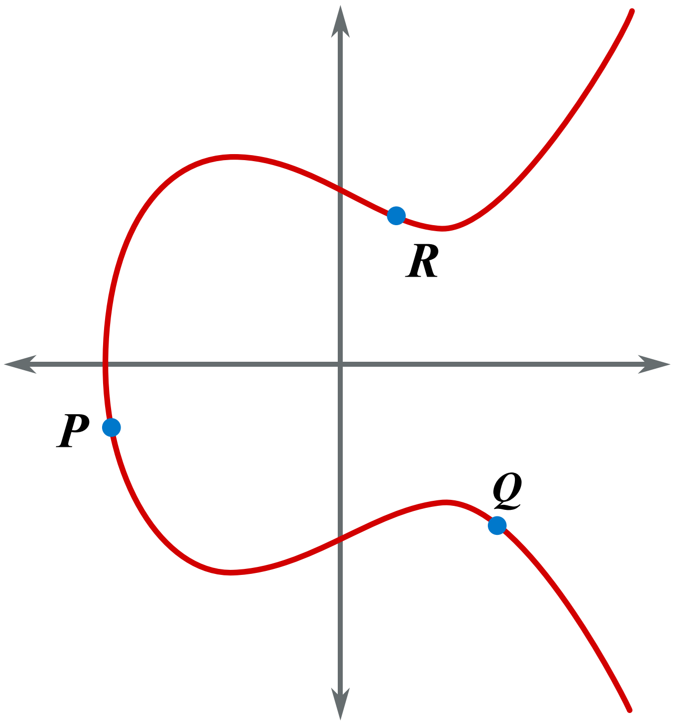
FA10 **(Distinct Additive and Multiplicative Identities)** $1 \neq 0$.

13. (a) (2 points) Let $\mathbb{F}$ be a field, and u a nonzero element of $\mathbb{F}$. Show that if $a \neq b$ for any $a, b \in \mathbb{F}$, then $ua \neq ub$.

(b) (3 points) Suppose $\mathbb{F}$ is a finite field containing q elements, and let 1 be the multiplicative identity. Prove that if u is a nonzero element of $\mathbb{F}$, then $u^{q-1} = 1$.

Hint: Use (a) and adapt our proof of Euler's theorem.

14. (2 points) Below is an elliptic curve over $\mathbb{R}$. Label the following points in the plane: $2Q$, $P+R$, and $-R$. **Show your work.**



15. (5 points) Let P be a point on an elliptic curve E, and let $n, k \in \mathbb{Z}$. State what it means for P to have *(additive) order* n. Prove that if P has order n, and $\gcd(n, k) = 1$, then kP also has order n.

16. Consider the equation $y^2 = x^3 + 43$ defined over $\mathbb{Z}/55\mathbb{Z}$, containing the point $P = (7, 34)$.

   (a) (1 point) Use the elliptic curve addition law to compute $2P$. Show your work. Note that $(68)^{-1} \equiv 17 \pmod{55}$.

   (b) (3 points) Factor $n = 55$ using the equation $y^2 = x^3 + 1$ and the point P. Show your work.

17. (4 points (bonus)) Find a polynomial $q(x)$ with integer coefficients with no rational roots, but satisfying the following property: $q(x)$ has a root in $\mathbb{Z}/p\mathbb{Z}$ for any prime p. In other words, for each prime p the equation $q(x) \equiv 0 \pmod{p}$ has a solution x. Prove your answer.

    Hint: It is possible to do this with a polynomial of the form $q(x) = (x^2-a)(x^2-b)(x^2-c)$ for suitably chosen integers a, b, c.