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" $\times$ 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.**

Since $35 = (5)(7)$, we can solve this equation by finding all solutions modulo 5 and modulo 7, then applying the Chinese Remainder Theorem. Our equation reduces to:

$$x^2 + 3x + 1 \equiv 0 \pmod{5} \qquad \text{and} \qquad x^2 + 0 + 3 \equiv 0 \pmod{7}$$

We could solve these two equations by simply plugging in all congruence classes modulo in $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/7\mathbb{Z}$, respectively, until we find the roots (if any exist). Alternatively, we can notice that if we choose suitable representatives of the coefficients, we can factor the polynomials over $\mathbb{Z}$:

$$\begin{aligned} x^2 + 3x + 1 &\equiv 0 \pmod{5} \\ x^2 - 2x + 1 &\equiv 0 \pmod{5} \\ (x-1)^2 &\equiv 0 \pmod{5} \end{aligned} \qquad \begin{aligned} x^2 + 3 &\equiv 0 \pmod{7} \\ x^2 - 4 &\equiv 0 \pmod{7} \\ (x-2)(x+2) &\equiv 0 \pmod{7} \end{aligned}$$

Because there are no zero divisors in $\mathbb{Z}/5\mathbb{Z}$, the only way that the product $(x-1)^2$ can be zero modulo 5 is if one of the factors $(x-1)$ is zero modulo 5, that is, if $x \equiv 1 \pmod{5}$. Similarly, the product $(x-2)(x+2)$ can only be zero modulo 7 if one of the factors is zero, so $x \equiv \pm 2 \pmod{7}$.

To find all solutions x modulo 35, we use the Chinese Remainder Theorem. First, using the Euclidean algorithm, we find integers u, v so that $5u + 7v = 1$.

$$\begin{aligned} 7 &= 5 + 2 \\ 5 &= 2(2) + 1 \end{aligned} \qquad \begin{aligned} 1 &= 5 - 2(2) \\ 1 &= 5 - 2(7-5) \\ 1 &= 3(5) - 2(7) \end{aligned}$$

Then the simultaneous system $x \equiv 1 \pmod{5}$ and $x \equiv 2 \pmod{7}$ has the solution:

$$3(5)(2) - 2(7)(1) \equiv 16 \pmod{35}$$

and the system $x \equiv 1 \pmod{5}$ and $x \equiv -2 \pmod{7}$ has the solution:

$$3(5)(-2) - 2(7)(1) \equiv -44 \equiv 26 \pmod{35}$$

and so we conclude that there are two solutions in $\mathbb{Z}/35\mathbb{Z}$, 16 and 26.

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.**

When p and q have a small difference, n is vulnerable to Fermat factorization. We compute $n + a^2$ for $a = 1, 2, 3, 4 \ldots$ until we find a perfect square. In this case, we notice that $n + 3^2 = 10000 = (100)^2$. Then, using the difference of squares formula:

$$\begin{aligned} n &= (100)^2 - 3^2 \\ n &= (100 + 3)(100 - 3) \\ n &= (103)(97) \end{aligned}$$

(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.

Since n divides the product $(639^2 - 3^2) = (639 - 3)(639 + 3)$, any prime factor of n must divide the factors 636 and 642. We choose one of these numbers use the Euclidean algorithm to compute its gcd with n:

$$\begin{aligned} 5671 &= 8(636) + 583 \\ 636 &= 583 + 53 \\ 583 &= 11(53) \end{aligned}$$

We find that $\gcd(636, 5671) = 53$, and we can factor $5671 = (53)(107)$.

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?

We choose the base $b = 2$, and factor $n - 1 = 220 = 2^2(55)$.

In order to compute powers of 2 modulo n, we compile a table:

$$\begin{aligned} 2^0 &\equiv 1 \pmod{n} \\ 2^1 &\equiv 2 \pmod{n} \\ 2^2 &\equiv 4 \pmod{n} \\ 2^4 &\equiv 16 \pmod{n} \\ 2^8 &\equiv 35 \pmod{n} \\ 2^{16} &\equiv 120 \pmod{n} \\ 2^{32} &\equiv 35 \pmod{n} \end{aligned}$$

So

$$2^{55} = 2^{32+16+4+2+1} \equiv (35)(120)(16)(4)(2)(1) \equiv 128 \pmod{221}$$

We let $b_0 \equiv 128 \pmod{221}$, and we iteratively square it.

$$b_1 = b_0^2 \equiv (128)^2 \equiv 30 \pmod{221}$$

Since 30 is not $\pm 1 \pmod{221}$, if $n = 221$ were prime, $b_1^2 \equiv 2^{n-1} \pmod{221}$ could not be 1 and so would violate Fermat's Little Theorem. We conclude that 221 must be composite.

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.**

We have the information we need to solve for the discrete logarithm of $42 = (2)(3)(7)$ using the index calculus.

$$\begin{aligned} 5^6 &\equiv (3)(7) \pmod{83} \\ 5^8 &\equiv 3^3 \pmod{83} \\ 5^{21} &\equiv (2^3)(3) \pmod{83} \end{aligned}$$

The second equation tells us that $8 \equiv 3L_5(3) \pmod{82}$. Since 3 is invertible modulo 82, this equation has a single possible solution for $L_5(3) \pmod{82}$, which we find by computing the inverse for 3:

$$\begin{aligned} 82 &= 3(27) + 1 \\ 1 &= 82 - 3(27) \end{aligned}$$

so $3^{-1} \equiv -27 \equiv 55 \pmod{82}$, and we can solve for

$$L_5(3) \equiv (55)(8) \equiv 30 \pmod{82}.$$

The third equation tells us that

$$\begin{aligned} 21 &\equiv 3L_5(2) + L_5(3) \pmod{82} \\ 3L_5(2) &\equiv 21 - 30 \pmod{82} \qquad \text{multiplying by } 3^{-1} \\ L_5(2) &\equiv 55(-9) \equiv 79 \pmod{82} \end{aligned}$$

The first equation tells us that $6 \equiv L_5(3) + L_5(7) \pmod{82}$. We could solve for $L_5(7) \pmod{82}$, but there's no need, since

$$L_5(42) \equiv L_5(2) + (L_5(3) + L_5(7)) \equiv 79 + 6 \equiv 3 \pmod{82}.$$

Since 5 is a primitive root, the integers congruent to $3 \pmod{82}$ are all integer solutions. We can easily verify our answer by computing $5^3 \pmod{83}$.

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

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

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

We can solve the discrete log problem using the baby step, giant step method. We see that the leftmost list gives numbers of the form $10^a \pmod{47}$ for integers $0 \leq a < 7$, and the rightmost list gives numbers of the form

$$(30) \cdot (33)^{7a} \equiv (30) \cdot (10^{-1})^{7a} \equiv (30) \cdot (10)^{-7a} \pmod{47}$$

for integers $0 \leq a < 7$.

We notice that 31 appears on both lists. Thus,

$$\begin{aligned} 10^5 &\equiv (30) \cdot (33^{14}) \pmod{47} \\ 10^5 &\equiv (30) \cdot (10^{-14}) \pmod{47} \\ 10^{19} &\equiv (30) \pmod{47}. \end{aligned}$$

The solutions are all integers x congruent to $19 \pmod{46}$.

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.

   The Hamming sphere of radius t around w is the closed ball of radius t in the Hamming metric centered at w, that is, it is the set of all words $\{v \mid d(v, w) \leq t\}$.

   (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.

   Let w be any word; we will show that w cannot be contained in both the Hamming sphere of radius t around u and the Hamming sphere of radius t around v. By the triangle inequality:

   $$2t + 1 \quad \leq \quad d(u, v) \quad \leq \quad d(u, w) + d(w, v)$$

   which means that at least one of the two distances $d(u, w)$ or $d(w, v)$ must be strictly greater than t, and so w can be contained in at most one of the two Hamming spheres.

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

   If a codeword v is transmitted but errors occur in up to t of its coordinates, then the resulting word will still be contained in the Hamming sphere of radius t around v. The triangle inequality shows that this word must strictly greater than distance t away from all other codewords; it cannot be contained in a Hamming sphere of radius t around any other codeword. Thus its unique nearest neighbour codeword is the original codeword v, and it can be accurately decoded.

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

A binary (7, 17, 3) would violate the Hamming Bound.

Assume a length-7 binary code with 17 codewords and minimal distance 3 did exist. Then since $3 \geq 2(1) + 1$, by the previous question we could place disjoint Hamming spheres of radius 1 around each codeword. Each of these balls would contain

$$\binom{7}{0} + \binom{7}{1} = 1 + 7 = 8$$

words in them. Because they are disjoint, the 17 Hamming spheres would collectively contain $(8)(17) = 136$ words. But there only $2^7 = 128$ binary length-7 words in total, so this code is impossible.

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.

Since C is 2-dimensional, it contains $2^2 = 4$ codewords, all vectors in the span of 10101 and 01001. These are:

$$C = \{00000, 10101, 01001, 11100\}.$$

The minimal distance of the code is equal to the minimal Hamming weight of the codewords; by inspection this is 2.

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

A parity check matrix for $G = [I_2\ P]$ is

$$H = [-P^T\ I_3] = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

The syndrome of v is

$$vH^T = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \end{bmatrix}$$

Since it is nonzero, we know v is not a codeword.

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

$$v + C = \{v + c \mid c \in C\} = \{10011, 00110, 11010, 01111\}$$

The coset leader is the word in $v + C$ with least Hamming weight; by inspection this is 00110.

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

The nearest codeword to v obtained by subtracting v from the coset leader in $v+C$. We get $00110 - 10011 = 10101$.

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.**

We use the Euclidean algorithm and polynomial division. Here I will use equal signs, even though all coefficients are understood to be congruence classes modulo 3.

$$
\begin{array}{rl}
 & x^2 - x + 3 \\
x+1 \;\big)\; & x^3 + 2x + 1 \\
 & -x^3 - x^2 \\
\hline
 & -x^2 + 2x \\
 & x^2 + x \\
\hline
 & 3x + 1 \\
 & -3x - 3 \\
\hline
 & -2
\end{array}
\qquad
\begin{array}{l}
x^3 + 2x + 1 = (x^2 + 2x)(x+1) + 1 \\
\\
\\
\\
1 = x^3 + 2x + 1 - (x^2 + 2x)(x+1) \\
1 = (x^3 + 2x + 1) + (-x^2 - 2x)(x+1) \\
1 = (x^3 + 2x + 1) + (2x^2 + x)(x+1)
\end{array}
$$

We conclude that $(x+1)^{-1} \pmod{P(x)} \equiv 2x^2 + x$.

It is easy to verify the answer by multiplying out $(x+1)(2x^2+x)$.

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.

False. This is true in general only when n and m are coprime.

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

True. Since 29 is prime, all 28 units satisfy this equation by Fermat's Little Theorem. The congruence class of zero does not satisfy the equation, so there are exactly 28 solutions.

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

False.

$$\begin{aligned}
\left(\frac{122}{1235}\right) &= \left(\frac{2}{1235}\right)\left(\frac{61}{1235}\right) \\
&= (-1)\left(\frac{61}{1235}\right) && \text{since } 1235 \equiv 3 \pmod 8 \\
&= (-1)\left(\frac{1235}{61}\right) && \text{since } 61 \equiv 1 \pmod 4 \\
&= (-1)\left(\frac{15}{61}\right) && \text{since } 1235 \equiv 15 \pmod{61} \\
&= (-1)\left(\frac{3}{61}\right)\left(\frac{5}{61}\right) \\
&= (-1)\left(\frac{61}{3}\right)\left(\frac{61}{5}\right) && \text{since } 61 \equiv 1 \pmod 4 \\
&= (-1)\left(\frac{1}{3}\right)\left(\frac{1}{5}\right) && \text{reducing modulo 3 and modulo 5} \\
&= (-1)(1)(1) = -1
\end{aligned}$$

(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.

True. If α is a primitive root, then the $\phi(n)$ units are exactly the powers of alpha

$$\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{\phi(n)} = 1.$$

Half of these powers are even, and these elements are evidently squares. The odd powers cannot be squares: if a unit α^m had a square root β, then we can express β as a power of α, say, $\beta \equiv \alpha^k \pmod{n}$, and

$$\alpha^m \equiv \beta^2 \equiv (\alpha^k)^2 \quad \Longleftrightarrow \quad m \equiv 2k \pmod{\phi(n)}.$$

Since $\phi(n)$ is even, this can happen only if m is even. Thus only the even powers of α 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.

True. Since b is not a multiple of 103, it is invertible modulo 103. If b and $-b$ were both squares, then their quotient $b(-b)^{-1} \equiv -1 \mod 103$ would also be a square. We proved that -1 is never a square modulo any prime congruent to 3 (mod 4). On the other hand, one of b and $-b$ must be a square, since we proved $b^{\frac{103+1}{4}} \equiv b^{26} \pmod{103}$ is a square root of either b or $-b$.

(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 $B = 5$.

False. For the $(p-1)$ algorithm to have a hope of succeeding, we need $(p-1)$ to divide $B!$. In this case, since 5! is not divisible by 9, 5! is not divisible by $(p-1)$. We need B at least 6.

(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.

True. The Miller-Rabin test can factor n only if $b_i \neq 1$ and $b_{i+1} \equiv b_i^2 \equiv 1 \pmod{n}$ at some step i with $0 < i < k-1$. In this case, $b_k \equiv b_{i+1}^{2^{k-i-1}} \equiv b^{n-1} \pmod{n}$ will necessarily also be 1; n is a Fermat pseudoprime for the base b.

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

True. Since $d(u,v) = wt(u-v)$, if codewords u and v realize the minimum distance d of the code C, then $(u-v)$ will have weight d. By linearity $u-v$ must also be a codeword.

(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.

False. Not all nonzero elements in this set have multiplicative inverses, for example, the integer 5 is in the set, but $\frac{1}{5}$ is not.

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.

We want an integer n so that $\phi(n) = 8$. The valid solutions are 15, 16, 20, 24, and 30.

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

An integer n cannot be a primitive root of any prime $p > 2$ if it is a perfect square, since then every unit would have a square root, which is impossible (citing, for example, properties of Legendre symbols, or Problem 10(d).) So integers $4, 9, 16, 25, \ldots$ are solutions.

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

By quadratic reciprocity, this can only be true when p is congruent to 3 (mod 4). So candidate solutions are $p = 11, 19, 23, 31, 43, 47, 51, 59 \ldots$

From here, we can search by trial and error for one of these primes p with $\left(\frac{7}{p}\right) = 1$.

Or, we can notice that the square units modulo 7 are 1, 4, and 2, so we want a prime p congruent to 3, 5, or 6 modulo 7. Solutions are $19, 31, 47, 59, \ldots$

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

This relationship will hold when p divides the difference

$$(21^2 - 10^2) = (21 - 10)(21 + 10) = (11)(31).$$

Equivalently, we know squares have at most two roots modulo a prime p, so this relationship can only hold when $10 \equiv \pm 21 \pmod{p}$

The two possible solutions are $p = 11$ and $p = 31$. .

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

A ternary linear code of dimension k will contain 3^k vectors. Since 6 is not a power of 3, no such code can exist.

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

A solution is any set of four length-3 binary vectors that are closed under linear combinations. For example,

$$C = \{000, 100, 010, 110\}.$$

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

We must choose 3 words of length 5 that all differ in all 5 positions. Using the alphabet $\mathbb{Z}/3\mathbb{Z}$, one solution are the words

$$C = \{00000, 11111, 22222\}.$$

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

Examples are any q-ary code of length 3 containing q^2 codewords. One example is the $[3, 2]$ binary code from part (f).

(i) A finite field of characteristic 6.

No such field can exist: we proved on the homework that the characteristic of a field must be a prime number. In this case, if a field had characteristic 6, then the field elements $(1+1)$ and $(1+1+1)$ would be (nonzero) zero divisors; these cannot exist in a field.

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

Let's choose an elliptic curve of the form $y^2 = x^3+bx+c$. The easiest way to generate an elliptic curve with known points is to choose b, then choose a point, then solve for c. Let's take $b \equiv 1 \pmod 5$ and choose the point $P = (1, 1)$. Solving, we find $c \equiv -1 \equiv 4 \pmod 5$. This curve contains the points $P = (1, 1)$ and $-P = (1, -1)$.

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)** $1 \neq 0$.

There are many ways to prove this result. Here is one possibility.

Proof. We first show that $(-1)\cdot(-1) + (-1) = 0$.

$$\begin{aligned}
(-1)\cdot(-1) + (-1) &= (-1)(-1) + (-1)(1) && \text{by definition of multiplicative identity} \\
&= (-1)(-1+1) && \text{FA9} \\
&= (-1)(0) && \text{by definition of multiplicative inverse,} \\
&= 0 && \text{by a result on the homework.}
\end{aligned}$$

Then, adding 1 to both sides of the equation $(-1)\cdot(-1) - 1 = 0$ gives

$$(-1)\cdot(-1) = 1, \qquad \text{as desired.}$$

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 $ua \neq ub$.

Suppose that $ua = ub$ for some nonzero element u in $\mathbb{F}$ and elements $a, b \in \mathbb{F}$. Since u has an inverse, we can multiply both sides by u^{-1} to conclude $a = b$. Thus whenever $a \neq b$, the products ua and ub cannot be equal.

(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.

Suppose that u is a nonzero element of $\mathbb{F}$, and let

$$a_1, a_2, \ldots, a_{q-1}$$

be a list of all nonzero elements of $\mathbb{F}$. By a result on the homework, fields contain no zero divisors, so the product ua_i will be nonzero for any i. By Part (a), the product ua_i will be distinct for each i, and so the list

$$ua_1, ua_2, \ldots, ua_{q-1}$$

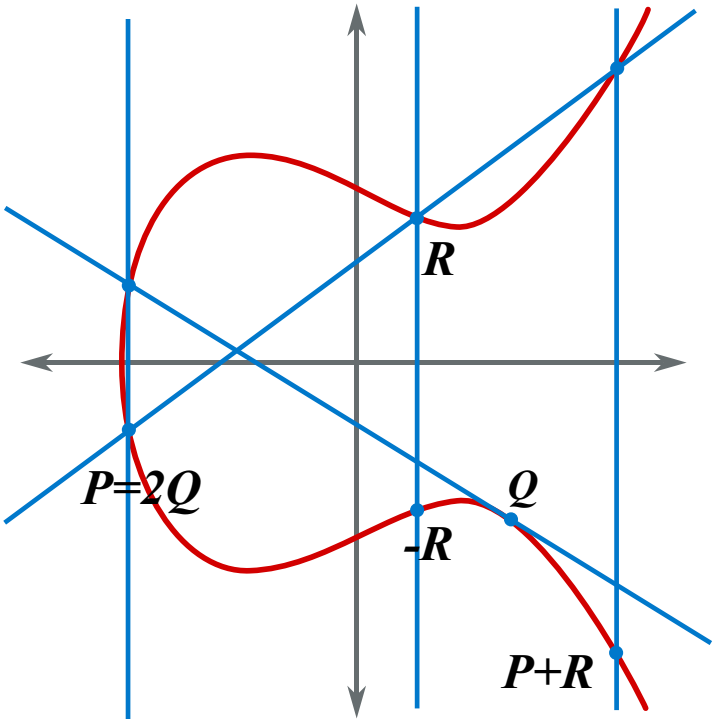
will again be a list of the $(q-1)$ nonzero elements of $\mathbb{F}$, each appearing exactly once, possibly in a different order. Thus, the products of all the elements in these two lists will be equal:

$$a_1 a_2 \cdots a_{q-1} = (ua_1)(ua_2) \cdots (ua_{q-1}) = u^{q-1} a_1 a_2 \cdots a_{q-1}$$

Here, we are using both associativity and commutativity of multiplication in a field. Since every element a_i has an inverse, we can multiply both sides of this equation by all the inverses of $a_1, a_2, \ldots a_{q-1}$ to find

$$1 = u^{q-1}.$$

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.

By definition, the *order* of a point Q on an elliptic curve is the smallest positive integer m so that $mQ = \infty$. So in this case n is the smallest positive integer such that $nP = \infty$.

To prove that kP has order n, we must show two things: that $n(kP) = \infty$, and that $\ell(kP) \neq \infty$ for an $0 < \ell < n$.

By definition,

$$kP = \underbrace{P + P + \cdots + P}_{k \text{ times}},$$

and

$$n(kP) = \underbrace{kP + kP + \cdots + kP}_{n \text{ times}} = (nk)P = k(nP),$$

so $n(kP) = k(nP) = k(\infty) = \infty + \infty + \cdots + \infty = \infty$ as desired. This shows that the order of kP is no greater than n.

Now suppose that $\ell(kP) = (\ell k)P = \infty$ for some $\ell \in \mathbb{Z}$. We can divide ℓk by n to write

$$(\ell k) = qn + r \qquad \text{for some remainder } 0 \leq r < n.$$

Then

$$\infty = \ell(kP) = (qn + r)P = q(nP) + rP = \infty + rP = rP.$$

Since $0 \leq r < n$ and n is the order of P, the remainder r must be zero.

It follows that $\ell k \equiv 0 \pmod{n}$. By assumption, k is coprime to n, and so has an inverse modulo n; multiplying through by $k^{-1} \pmod{n}$ we see that $\ell \equiv 0 \pmod{n}$.

The smallest positive residue of 0 modulo n is the integer n. We conclude that n is the smallest positive integer such that $n(kP) = \infty$, and therefore n is the order of kP.

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 $(68)^{-1} \equiv 17 \pmod{55}$.

Using the formula for the addition law for $P + P = (x_3, y_3)$

$$m \equiv \frac{3(x^2) + b}{2y} \equiv (3(7^2) + 0)(2(34))^{-1} \equiv (147)(17) \equiv 24 \pmod{55}$$

$$x_3 \equiv m^2 - 2x \equiv 24^2 - 2(7) \equiv 12 \pmod{55}$$

$$y_3 \equiv m(x - x_3) - y \equiv 24(7 - 12) - 34 \equiv 11 \pmod{55}$$

So we have $(7, 34) + (7, 34) = (12, 11)$ on the curve.

(b) (3 points) Factor $n = 55$ using the equation $y^2 = x^3 + 43$ and the point P. Show your work.

We will compute multiples of P in hopes of finding a slope m with a denominator that is not invertible modulo 55.

$$3P = P + 2P = (7, 34) + (12, 11)$$

First we compute the slope m:

$$m = \frac{y_2 - y_1}{x_2 - x_1} \equiv (11 - 34)(12 - 7)^{-1} \equiv (32)(5)^{-1} \pmod{55}$$

But when we use the Euclidean algorithm to attempt to invert 5 (mod 55), we find that $\gcd(5, 55) = 5$, and we are able to factor $55 = (5)(11)$.

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.

One solution is the polynomial $q(x) = (x^2-2)(x^2-3)(x^2-6)$. None of the integers $2, 3$, or 6 is a square, so this polynomial has no rational roots.

However, we can show for any prime p, at least one of 2, 3, and 6 must be a square modulo p, and so its square root will be a root of the polynomial modulo p. The crucial feature is that $6 = (2)(3)$.

If the prime p is 2 or 3, then $x = 0$ is a solution.

If the prime p is not 2 or 3, then 2, 3, and 6 are all units modulo p. One way to proceed is to cite the primitive root theorem, and express 2 and 3 as powers of a primitive root α. If they are both non-squares and have odd exponents, then their product will have an even exponent and necessarily be a square.

Equivalently, we can use properties of the Legendre symbols:

$$\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$$

If neither 2 nor 3 is a square modulo p, then $\left(\frac{2}{p}\right)$ and $\left(\frac{3}{p}\right)$ will both be -1; their product will be 1 and 6 must be a square modulo p.