Name and UNI:

**Making, Breaking Codes, Midterm 2**

This examination booklet contains 6 problems. Do all of your work on the pages of this exam booklet. Show all your computations and justify/explain your answers. Cross out anything you do not want graded.

If there is a mistake in the question or if you are not sure what something means, just make a guess, explain what is going on in your answer, and continue.

You have about 75 minutes to complete the midterm. Do not begin until instructed to do so. When time is up, stop working and close your test booklet. Books, notes, calculators, cell phones, headphones, laptops, and other electronic devices are not allowed.

**1.** You are given that 350 and 147 have the same square modulo 2059. Use this information to find a factor of 2059. Show your work.

Since 350 and 147 have the same square modulo 2059 we know that $350^2 - 147^2$ is zero modulo 2059. Thus we get that $(350 - 147)(350 + 147)$ is divisible by 2059. Thus it is likely that $203 = 350 - 147$ and 2059 have a factor in common. Therefore it makes sense to compute

$$\gcd(203, 2059) = \gcd(203, 29) = 29$$

The first equality because $2059 = 10 * 203 + 29$ and the second because 29 divides 203. Thus 29 is a divisor of 2059 and the we are done answering the question.

**2.** You are given that $P = X^7 + X^3 + X^2 + X + 1$ in $\mathbf{F}_2[X]$ is an irreducible polynomial with coefficients in the field $\mathbf{F}_2$ with 2 elements.
**(a)** What is a multiplicative inverse of $X$ modulo $P$?

Since we have

$$P = X^7 + X^3 + X^2 + X + 1 = X(X^6 + X^2 + X + 1) + 1$$

we see immediately that the inverse of $X$ mod $P$ is $X^6 + X^2 + X + 1$ mod $P$.

**(b)** Compute the multiplicative inverse of $X^2$ modulo $P$.

Method I: the inverse of $X^2$ is the square of the inverse of $X$. Hence we get

$$(X^6 + X^2 + X + 1)^2 = X^{12} + X^4 + x^2 + 1$$

because we are working modulo 2. Then we have

$$\begin{aligned} X^{12} &= X^5 X^7 \\ &= X^5(X^3 + X^2 + X + 1) \\ &= X^8 + X^7 + X^6 + X^5 \\ &= (X+1)(X^3 + X^2 + X + 1) + X^6 + X^5 \\ &= X^6 + X^5 + X^4 + 1 \bmod P \end{aligned}$$

and hence the final answer is

$$X^6 + X^5 + X^4 + 1 + X^4 + X^2 + 1 = X^6 + X^5 + X^2$$

Method II: we can use the Euclidean algorithm as follows:

$X^7+X^3+X^2+X+1 = (X^5+X+1)X^2+X+1 \quad \text{and} \quad X^2 = (X+1)(X+1)+1$

Doing backsubstitution we get

$1 = X^2+(X+1)(X+1) = X^2+(X+1)(X^5+X+1)X^2+(X+1)(X^7+X^3+X^2+X+1)$

and hence we get that the inverse is

$$1 + (X+1)(X^5 + X + 1) = X^6 + X^5 + X^2$$

Method III: we can use the following trick

$(X^2)^{-1} = X^{-1}(X^6+X^2+X+1) = X^5+X+1+X^{-1} = X^5+X+1+X^6+X^2+X+1 = X^6+X^5+X^2 \bmod P$

where we have used the result gotten in (a) twice.

**3.** A trusted authority has published a large integer $n$ which is secretly the product of two distinct large primes. Moreover, they publish an integer $y$ mod $n$. Peggy claims she knows a square root $s$ of $y$ mod $n$. Explain a protocol that allows Peggy to convince Victor she indeed knows a square root of $y$ mod $n$ without giving away any information about this square root.

**Step 1**: Peggy chooses a random number $r_1$ and computes $r_2 \equiv sr_1^{-1} \pmod{n}$. Then she computes $x_1 \equiv r_1^2 \pmod{n}$ and $x_2 \equiv r_2^2 \pmod{n}$ and sends $x_1, x_2$ to Victor.

**Step 2:** Victor verifies that $x_1 x_2 \equiv y \pmod{n}$. If this is the case, then he chooses one of $x_1, x_2$ and asks Peggy to give a square root of it. Then he verifies if it is actually a square root.

**Step 3:** Repeat the above steps several times until Victor is convinced.

**4.** Fields.
**(a)** State the definition of a field.

A field is a set $F$ which comes with two special elements 0 and 1 and comes with an addtion $+$ and a multiplication $\cdot$ such that the following are true:

1. addition and multiplication are associative and commutative,
2. the distributive law holds $x \cdot (y + z) = x \cdot y + x \cdot z$ for all $x, y, z \in F$,
3. $0 + x = x$ for all $x \in F$,
4. every $x \in F$ has an additive inverse $-x$ such that $x + -x = 0$,
5. $1 \cdot x = x$ for all $x \in F$,
6. every **nonzero** $x \in F$ has a multiplicative inverse $x^{-1}$ such that $x \cdot x^{-1} = 1$.

**(b)** Construct a field with 9 elements.

In the course it was explained that $\mathbf{F}_3[X]$ mod $P$ is a field with $3^2 = 9$ elements if $P$ is an irreducible monic polynomial of degree 2 in $\mathbf{F}_3[X]$. Take $P = X^2 + 1$ for example. It is irreducible as $P$ has no roots in $\mathbf{F}_3$ because $P(0) = 1$, $P(1) = 2$, and $P(-1) = 2$.

**5.** Factoring integers using elliptic curves. Let $n$ be an integer.
**(a)** Explain the steps of the algorithm to factor $n$ using elliptic curves.

**Step 1:** Choose $x_0, y_0, b \in \mathbb{Z}_n$ *randomly.* Then compute

$$c \equiv y_0^2 - x_0^3 - bx_0 \pmod{n}.$$

Thus we have an elliptic curve

$$E : y^2 \equiv x^3 + bx + c \pmod{n}$$

with the point $P = (x_0, y_0)$ lying on $E$.

**Step 2:** Choose a reasonable bound $B$ that consists of small prime factors.

**Step 3:** Compute $B \cdot P \pmod{n}$ by using the addition formula of elliptic curves.

**Step 4:** Suppose during the computation of $B \cdot P \pmod{n}$, the slope of a chord (or tangent) is a rational number of the form $u/v$ with

1. $1 < gcd(v, n) < n$. Then stop and output $gcd(v, n)$. This gives a prime factor of $n$;
2. $\gcd(v, n) = n$. Then go back to **Step 1** (i.e., try a new curve with a new point on it).
3. $\gcd(v, n) = 1$. Then continue the computation of $B \cdot P \pmod{n}$.

**Step 5:** If we can compute $B \cdot P \pmod{n}$ successfully, then go back to **Step 1**.

**(b)** Why is this factoring method more likely to succeed than Pollard's $p - 1$ factoring algorithm?

For Pollard's $(p - 1)$ method, if the procedures fail to give a prime divisor, the only way is to increase the size of the bound $B$ and retry. If $p - 1$ consists of a large prime factor, this process is very inefficient!

For the Elliptic Curve Method, one can carry out the algorithm for *various* elliptic curves. Suppose $n = pq$, where $p, q$ are two distinct prime numbers. Among a large collection of elliptic curves $E$, *heuristically* the order of the group $E(\mathbb{F}_p)$ varies *randomly* in the range

$$[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$$

and it is likely that there exists $E$ such that $|E(\mathbb{F}_p)|$ consists of solely small prime factors. Thus, there is a high chance that $|E(\mathbb{F}_p)|$ divides the chosen bound $B$ and so $B \cdot P = \infty \pmod{p}$. Similar discussion holds for $E(\mathbb{F}_q)$. This establishes a huge contrast with Pollard's $(p - 1)$ method!

Moreover, one expects that $p, q$ act independently and it is likely to encounter some $k \leq B$ such that $kP = \infty \pmod{p}$ but $kP \neq \infty \pmod{q}$ (or vice versa). In this case, the Elliptic Curve Method outputs a prime factor of $n$ successfully.

**6.** You are given that $P = X^4 + X^3 + X^2 + X + 1$ in $\mathbf{F}_2[X]$ is an irreducible polynomial with coefficients in the field $\mathbf{F}_2$ with 2 elements. Let $\mathbf{F}_{2^4}$ be the field defined by $P$ and denote $\omega$ the element of this field determined by $X$. Let

$$E : y^2 + y = x^3 + x + 1$$

be the elliptic curve over $\mathbf{F}_{2^4}$
**(a)** Show that $P_1 = (\omega, \omega^2 + 1)$ is a point on $E$.

Substituting $x = \omega$ and $y = \omega^2 + 1$ into the equation for $E$ we have to show that

$$(\omega^2 + 1)^2 + (\omega^2 + 1) = \omega^3 + \omega + 1$$

in our field. This is true because this equation is equivalent to

$$\omega^4 + 1 + \omega^2 + 1 = \omega^3 + \omega + 1$$

which in turn is equivalent to

$$\omega^4 + \omega^3 + \omega^2 + \omega + 1 = 0$$

which is true because we are working modulo the polynomial $P$ and $\omega$ corresponds to $X$.

**(b)** Compute the equation of the line $L$ through $P_1$ and $P_2 = (\omega+1, \omega^2+\omega+1)$.

The slope of $L$ is gotten by taking the difference of the $y$-coordinates and dividing by the difference of the $x$ coordinates. Thus the slope is $(\omega^2 + \omega + 1 - (\omega^2 + 1))/(\omega+1-\omega) = \omega$. Since $L$ passes through $P_1$ we must have the line $y = \omega x+1$.

**(c)** You are given that $P_2$ is also a point on $E$. Find the third point on the line $L$ which lies on $E$.

We fill in the equation of the line $L$ into the equation for $E$. Then we find

$$(\omega x + 1)^2 + \omega x + 1 = x^3 + x + 1$$

This is equivalent to

$$x^3 + \omega^2 x^2 + (\omega + 1)x + 1 = 0$$

We know that the $x$-coordinates of $P_1$ and $P_2$ are solutions and hence we see that the third solution satisfies

$$\omega + (\omega + 1) + \text{third solution} = \omega^2$$

by looking at the coefficient of $x^2$ in the polynomial equation above. Hence this gives $x = \omega^2 + 1$ and substituting into the equation for $L$ we obtain

$$y = \omega(\omega^2 + 1) + 1 = \omega^3 + \omega + 1$$