MATH 195: TAKE HOME FINAL

JOHN VOIGHT

Problem A1. *Alice, Bob, Chris, and Eve communicate over a public network. They encrypt all messages they send using the RSA system. Bob and Chris have the same public modulus $n_B = n_C$, but different public encryption exponents: $e_B \neq e_C$.*

(a) *Show how Bob can decipher all messages sent to Chris.*
(b) *Suppose that $\gcd(e_B, e_C) = 1$, and that Alice sends the same secret message to Bob and to Chris. Show how Eve can decipher the message.*

Solution. For (a), since Bob knows $n_B = n_C = n$, he knows the factorization $n = pq$ and $\phi(n) = (p-1)(q-1)$. (This is how n is constructed, starting from p, q.) By the (extended) Euclidean algorithm, Bob can compute $d_C = e_C^{-1} \pmod{\phi(n)}$, and thereby decrypt all messages. (It also suffices to do this computation modulo $\ell = \operatorname{lcm}(p-1, q-1)$.)

Note: The algorithm which given m such that $a^m = 1 \pmod{n}$ for all n factors n is not applicable in this situation: it is far too slow!

For (b), note that since $\gcd(e_B, e_C) = 1$, there are integers m_B, m_C such that $e_B m_B + e_C m_C = 1$. Therefore given the encrypted messages $y_B = x^{e_B} \pmod{n}$ and $y_C = x^{e_C} \pmod{n}$ for plaintext x, Eve computes

$$y_B^{m_B} y_C^{m_C} = x^{m_B e_B + m_C e_C} = x \pmod{n}.$$

Eve does this without ever computing d_B or d_C!

Problem A2.

(a) *How many monic irreducible polynomials in $\mathbb{F}_5[X]$ of degree 3 are there?*
(b) *Given an explicit construction of the field $\mathbb{F}_{125}$.*
(c) *Pick, in the field that you constructed in* (b)*, an element that does not belong to $\mathbb{F}_5$, and compute its inverse.*

Solution. For (a), we use the formula from class: We let

$$a_n(p) = \#\{f \in \mathbb{F}_p[X] : f \text{ monic, irreducible, } \deg f = n\}.$$

We then have:

$$a_n(p) = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d}$$

where $\mu(d)$ is the Möbius function (0 if d is divisible by a square, otherwise $(-1)^r$ if d is the product of r distinct primes). From this we find

$$a_3(5) = \frac{1}{3} \sum_{d|3} \mu(d) 5^{n/d} = \frac{1}{3}(5^3 - 5) = 40.$$

Date: May 21, 2002.

It is a theorem that if $f(X)$ is an irreducible polynomial of degree 3 over $\mathbb{F}_5$, then $\mathbb{F}_5[X]/(f(X))$ is a field of $5^3 = 125$ elements. It suffices to find one of these 40 irreducible polynomials. The polynomial $f(X) = X^3 + X + 1$ has no roots (try successively $X = 0, 1, \ldots, 4$); if it were reducible, it would have to have a linear factor (hence a root), so it is irreducible. Therefore

$$\mathbb{F}_{125} \simeq \mathbb{F}_5[X]/(X^3 + X + 1).$$

For (c), we compute X^{-1}. One can do this using the extended Euclidean algorithm, or by solving the equation $X(aX^2 + bX + c) = 1 \pmod{X^3 + X + 1}$ for a, b, c, but here is a simpler method: since $X^3 + X + 1 = 0$, we have

$$-(X^3 + X) = X(-X^2 - 1) = 1.$$

Therefore $X^{-1} = -X^2 - 1$.

Problem A3. *Let the elliptic curve E over $\mathbb{F}_2$ be defined by the equation*

$$y^2 + y = x^3 + x.$$

(a) *List all points of $E(\mathbb{F}_2)$.*
(b) *Make a table showing $P + Q$ for all $P, Q \in E(\mathbb{F}_2)$. Explain how you made the table. (Avoid performing too many additions.)*
(c) *How many elements does $E(\mathbb{F}_4)$ have?*

Solution. For (a), we have the points $E(\mathbb{F}_2) = \{(0,0), (1,0), (0,1), (1,1)\} \cup \{O\}$.

For (b), we note that $E(\mathbb{F}_2)$ is a group, so since it is of prime order it is cyclic. It suffices to compute the powers of a single generator $P = (0,0)$. We first use the negative formula:

$$-P = (x, -y - a_1 x - a_3) = (x, y + 1);$$

This says that $-(0,0) = (0,1) = 4P$ (since $5P = O$, this is a group of order 5) and $-(1,0) = (1,1)$. We now only need to decide which of these is $2P$ and which is $3P$.

We compute $2P$: Let $f = y^2 + y + x^3 + x$. Then the tangent line to f at $P = (0,0)$ is obtained by implicitly differentiating f with respect to x:

$$2y\frac{dy}{dx} + \frac{dy}{dx} + 3x^2 + 1 = 0$$

so

$$\left.\frac{dy}{dx}\right|_{(0,0)} = x^2 + 1\big|_{(0,0)} = 1.$$

This line goes through $P = (0,0)$, so it is $y = x$. This line intersects E at

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

so also at $x = 1$, and hence $y = x = 1$. We then take its negative, which is the point $2P = (1,0)$.

Therefore $2P = (1,0)$, and we have an isomorphism

$$E(\mathbb{F}_2) \simeq \mathbb{Z}/5\mathbb{Z} = \langle P \rangle = \{O, (0,0), (1,0), (1,1), (0,1)\}.$$

This gives us the following table:

$+$	O	$(0,0)$	$(1,0)$	$(1,1)$	$(0,1)$
O	O	$(0,0)$	$(1,0)$	$(1,1)$	$(0,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(1,1)$	$(0,1)$	O
$(1,0)$	$(1,0)$	$(1,1)$	$(0,1)$	O	$(0,0)$
$(1,1)$	$(1,1)$	$(0,1)$	O	$(0,0)$	$(1,0)$
$(0,1)$	$(0,1)$	O	$(0,0)$	$(1,0)$	$(1,1)$

For (c), we invoke Hasse's theorem (second version) from class:

$$\#E(\mathbb{F}_{2^n}) = 2^n + 1 - t_n$$

where $t_n = \pi^n + \overline{\pi}^n$ for some $\pi \in \mathbb{C}$ with $|\pi| = \sqrt{2}$. This gives us the equations $\pi\overline{\pi} = 2$ and

$$\pi + \overline{\pi} = 2 + 1 - \#E(\mathbb{F}_2) = -2$$

for which we find $\pi^2 + 2\pi + 2 = 0$, or $\pi = -1 \pm i$. Therefore

$$\#E(\mathbb{F}_4) = 4 + 1 - ((-1+i)^2 + (-1-i)^2) = 5 + 0 = 5.$$

Note that all of the points of $E(\mathbb{F}_4)$ are defined over $\mathbb{F}_2$!

Problem B1. *This problem is about a monoalphabetic cipher. Throughout, the English alphabet is identified with $\mathbb{Z}/26\mathbb{Z}$ by $A = 0$, $B = 1$, ..., $Y = 24$, $Z = 25$. The encryption function is*

$$\begin{aligned} \varepsilon : \mathbb{Z}/26\mathbb{Z} &\to \mathbb{Z}/26\mathbb{Z} \\ \varepsilon(x) &= \alpha x + \beta \qquad (x \in \mathbb{Z}/26\mathbb{Z}) \end{aligned}$$

for certain secret numbers α, $\beta \in \mathbb{Z}/26\mathbb{Z}$. For example, if $\alpha = 5$ and $\beta = 10$ then H is encrypted as T, because $H = 7$ and $\varepsilon(7) = 5 \cdot 7 + 10 = 19 = T$.

Suppose now that a very long English plaintext is encrypted by means of the cipher, and that W is the most frequent letter in the ciphertext.

(a) *What is probably the third most frequent letter in the ciphertext? [Use the table of letter frequencies from the textbook.]*
(b) *Suppose that B is the second most frequent letter in the ciphertext. What are the most likely values for α and β?*
(c) *Suppose that α, β are as you guessed in* (b). *Show that to decrypt a ciphertext it suffices to encrypt it twice in succession. [If you guessed wrong in* (b) *this may be false. In that case, change your guess.]*

Solution. The most frequently used letter is $E = 4$, and since $W = 22$, we guess that $\varepsilon(4) = 4\alpha + \beta = 22$. The third most frequently used letter is $R = 17$, so we wish to find the value of $\varepsilon(17) = 17\alpha + \beta \pmod{26}$. Notice that

$$17\alpha + \beta \equiv 4\alpha + \beta \equiv 9 \pmod{13}$$

so already $\varepsilon(17) = 9$ or 22, but the latter cannot occur since the map ε is a bijection. Therefore the most frequent letter in the ciphertext is likely to be $J = 9$.

For (b), we note that the second most frequently used letter is $T = 19$, since $W = 22$ and $B = 1$, we guess that $\varepsilon(4) = 22$ and $\varepsilon(19) = 1$. This gives the two

equations

$$4\alpha + \beta = 22$$
$$19\alpha + \beta = 1$$

Subtracting these gives $15\alpha = -21 = 5 \pmod{26}$, so since $15^{-1} = 7 \pmod{26}$ (you can compute this using the Euclidean algorithm, or by trying out values), $\alpha = 7 \cdot 5 \equiv 9 \pmod{26}$. Therefore $\beta = 22 - 36 \equiv 12 \pmod{26}$, and $\varepsilon(x) = 9x + 12$.

For (c), we need to show that $\varepsilon^{-1}(x) = \varepsilon^2(x)$, i.e. $\varepsilon^3(x) = x$. This is easily verified:

$$\varepsilon^3(x) = 9(9(9x + 12) + 12) + 12 = 729x + 1092 \equiv x \pmod{26}.$$

Problem B2. *Let* $\mathbb{F}_{256} = \mathbb{F}_2[X]/(X^8 + X^4 + X^3 + X + 1)$*, and let* $B : \mathbb{F}_{256} \to \mathbb{F}_{256}$ *be the substitution used by Rijndael (see the class notes on the web page,* 04/02/02–04/04/02*). Find elements* u*,* $v \in \mathbb{F}_{256}$ *with* $B(u) = v$ *and* $B(v) = u$*. [You may want to use a computer for this purpose.]*

Solution. First, we define $A : \{f \in \mathbb{F}_2[X] : \deg f < 8\}$ to itself by

$$A(f) \equiv (X^4 + X^3 + X^2 + X + 1)f + (X^6 + X^5 + X + 1) \pmod{X^8 + 1}.$$

We define $B : \mathbb{F}_{256} \to \mathbb{F}_{256}$ by

$$B(a) = \begin{cases} A(a^{-1}), & a \neq 0, a^{-1} \text{ computed in } \mathbb{F}_{256}; \\ A(0), & a = 0. \end{cases}$$

The following Maple script will compute this encipherment:

```
# This function takes as input a number n = 0..255, converts it
# to binary and then a polynomial by
#   n = b7...b0 |-> b7*X^7 + ... + b0 = f.
# It then computes the Rijndael function
#   B(f) = A(f^(-1)) (unless f = 0, and then B(0)=A(0))
# where
#   A(f) = (X^4+X^3+X^2+X+1)f + (X^6+X^5+X+1) mod(X^8+1).
# It returns the decimal value of the answer using the bijection
# defined above.
# To see the intermediate output, uncomment the print lines.

m := X^8 + X^4 + X^3 + X + 1:

rijn := proc(p) local b,f,s,t,i,n;
  n := p mod 256;

  # Convert number to polynomial
  f := 0;
  for i from 1 to 8 do
    f := f + ((n mod 2^i) - (n mod 2^(max(i-1,0))))/
                              2^(i-1)*X^(i-1);
  od;
#  print(f);
```

```
  # Compute inverse by the extended Euclidean algorithm
  if ( f <> 0 ) then
    gcdex(f,m,X,'s','t');
    f := s mod 2;
  fi;
#  print(f);

  # Compute Alpha
  f := rem((X^4+X^3+X^2+X+1)*f + X^6+X^5+X+1,X^8+1,X) mod 2;
#  print(f);

  # Convert back to decimal
  b := subs(X=2,f);
  b;
end:
```

The following script will then find a 2-cycle:

```
for n from 0 to 255 do
  if( rijn(rijn(n)) = n ) then
    print(n);
  fi;
od;
```

The output is $115, 143$, which corresponds to the polynomials

$$115 = 73 = 01110011 = X^6 + X^5 + X^4 + X + 1$$

and

$$143 = 85 = 10000101 = X^7 + X^3 + X^2 + X + 1.$$

We verify this by hand: We compute

$$(X^6 + X^5 + X^4 + X + 1)^{-1} = X^7 + X^2 + 1$$

and

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

and similarly

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

and

$$A(X^7 + X^5 + X^2) = X^6 + X^5 + X^4 + X + 1.$$

In fact, one can compute the complete cycle decomposition; to find the cycle containing 0 and its order, we list:

```
C0 := [0];
while ( op(nops(C0),C0) <> op(1,C0) or nops(C0) = 1 ) do
  C0 := [op(C0),rijn(op(nops(C0),C0))];
od:
C0 := [op(1..(nops(C0)-1),C0)];
nops(C0);
```

This outputs the 59-cycle:

$$(0, 99, 251, 15, 118, 56, 7, 197, 166, 36, 54, 5, 107, 127, 210, 181, 213, 3, 123, 33, 253, 84, 32, 183, 169, 211, 102, 51, 195, 46, 49, 199, 198, 180, 141, 93, 76, 41, 165, 6, 111, 168, 194, 37, 63, 117, 157, 94, 88, 106, 2, 119, 245, 230, 142, 25, 212, 72, 82)$$

Using the command `sort(C)`, we see that the next value is 1, which belongs to an 81-cycle:

$$(1, 124, 16, 202, 116, 146, 79, 132, 95, 207, 138, 126, 243, 13, 215, 14, 171, 98, 170, 172, 145, 129, 12, 254, 187, 234, 135, 23, 240, 140, 100, 67, 26, 162, 58, 128, 205, 189, 122, 218, 87, 91, 57, 18, 201, 221, 193, 120, 188, 101, 77, 227, 17, 130, 19, 125, 255, 22, 71, 160, 224, 225, 248, 65, 131, 236, 206, 139, 61, 39, 204, 75, 179, 109, 60, 235, 233, 30, 114, 64, 9)$$

We repeat to get the following remaining cycles, of length 87 and 27:

$$(4, 242, 137, 167, 92, 74, 214, 246, 66, 44, 113, 163, 10, 103, 133, 151, 136, 196, 28, 156, 222, 29, 164, 73, 59, 226, 152, 70, 90, 190, 174, 228, 105, 249, 153, 238, 40, 52, 24, 173, 149, 42, 229, 217, 53, 150, 144, 96, 208, 112, 81, 209, 62, 178, 55, 154, 184, 108, 80, 83, 237, 85, 252, 176, 231, 148, 34, 147, 220, 134, 68, 27, 175, 121, 182, 78, 47, 21, 89, 203, 31, 192, 186, 244, 191, 8, 48)$$

and

$$(11, 43, 241, 161, 50, 35, 38, 247, 104, 69, 110, 159, 219, 185, 86, 177, 200, 232, 155, 20, 250, 45, 216, 97, 239, 223, 158).$$

Note that $59 + 81 + 87 + 27 = 254$, the numbers remaining from these lists, $115, 143$, form the lone 2-cycle.

Problem B3. *Let $p = 2^{16} + 1 = 65537$. This is a prime number (you do not need to prove this).*

(a) *What is the order of 3 in the group $\mathbb{F}_p^*$? Is 3 a primitive root modulo p?*
(b) *What is the order of 2 in the group $\mathbb{F}_p^*$? Prove that $\log_3 2$ is divisible by 2^{11}.*
(c) *Compute $\log_3 2$. Which method do you use? Show your work.*

Solution. Notice that $p - 1 = 2^{16}$. Therefore if we check that $3^{2^{15}} \not\equiv 1 \pmod{p}$, then the order of 3, which divides 2^{16} (because it is the order of the group), does not divide 2^{15} (by this calculation), so it must be equal. (Recall this is a special case of a theorem from class regarding the prime divisors of $p - 1$.)

By repeated squaring, we compute

$$3^2 = 9,\ 3^4 = 9^2 = 81, \dots, 3^{2^{11}} = -32, \dots, 3^{2^{15}} \equiv -1 \pmod{p}.$$

Therefore 3 is indeed a primitive root, and has order 65536.

For (b), note that again the order of 2 divides 2^{16}, so it is the smallest integer such that $2^{2^m} \equiv 1 \pmod{p}$. Since $2^{16} \equiv -1 \pmod{2^{16}+1}$, and all other values are too small, we conclude that 2 has order 32. Let $m = \log_3 2$: then $3^m \equiv 2 \pmod{p}$. But we just found that 32 is order of 2, so

$$(3^m)^{32} = 3^{32m} \equiv 2^{32} \equiv 1 \pmod{p}.$$

Therefore the order of 3 divides $32m$, hence $2^{16} \mid 2^5 m$, or $2^{11} \mid m = \log_3 2$.

For (c), one can compute the discrete logarithm using baby step-giant step, or by using the Pollig-Hellman technique. We opt for an ad hoc method, involving trickery (forgive us, please): by repeated squaring in the above, we found that $3^{2^{11}} = -8 = -2^3$. We also know that $2^{16} \equiv -1 \pmod{65537}$, so

$$3^{2^{11}} \equiv 2^{16} 2^3 = 2^{19} \pmod{65537}.$$

Recall that the order of 2 is 32, so we compute $19^{-1} \equiv 27 \pmod{32}$, and

$$(3^{2^{11}})^{27} = 3^{27 \cdot 2^{11}} \equiv (2^{19})^{27} \equiv 2 \pmod{65537}.$$

This says that $\log_3 2 = 27 \cdot 2^{11} = 55296$.

Problem B4. *Analyse the complexity of the Pohlig-Hellman method for computing discrete logarithms (see the class notes on the web page,* 04/18/02–04/25/02*). More precisely, give upper bounds both for the number of bit operations performed by the algorithm and for the number of operations in the group. These upper bounds should be expressed as functions of the numbers m_1, m_2, ..., m_t that form part of the input. (Do keep the* ***Important note*** *on the cover page in mind.)*

Solution. First, we analyze baby step-giant step:

(1) Pick a positive integer M with $M^2 \geq m = \mathrm{ord}(g)$, e.g. $\lceil \sqrt{m} \rceil$.
(2) Compute
$$h, hg, hg^2, \ldots, hg^{M-1}$$
(the baby steps) and
$$g^M, g^{2M}, \ldots, g^{M^2}$$
(the giant steps).
(3) If we find two elements in common, then $hg^i = g^{jM}$, so $h = g^{jM-i}$ and $\log_g h = jM - i$, and otherwise $\log_g h$ doesn't exist.

This requires no more than $M - 1$ group operations for the baby steps. For the giant steps, we use repeated squaring to compute g^M, which requires no more than

$$2k = 2\lfloor \frac{\log M}{\log 2} \rfloor$$

group operations. We then require $M - 1$ group operations to fill out the powers, for a total of no more than $2M + 2\log M / \log 2$ operations. Finally, to compare lists, keeping the lists sorted gives us a comparison which takes time no more than $2M$ bit operations (we go once through one list and keep track of where we are on the other).

Now the Pohlig-Hellman method runs as follows:

(1) Compute $m' = m_1 m_2 \ldots m_{t-1} = m/m_t$.
(2) Use the baby step-giant step method (or complete enumeration) to find $a = \log_{g^{m'}} h^{m'}$. If it doesn't exist, then $\log_g h$ doesn't exist either, and the algorithm stops.
(3) Compute hg^{-a}.
(4) Use the Pohlig-Hellman method with input
$$G,\ g^{m_t},\ m' = m_1 m_2 \ldots m_{t-1},\ hg^{-a},$$

to compute $b = \log_{g^{m_t}}(hg^{-a})$. Output $\log_g h = m_t b + a$ if b exists, and if it does not, then the $\log_g h$ does not exist either.

The first step requires $t-1$ bit operations. Baby step-giant step requires

$$2\lceil\sqrt{m_t}\rceil + 2\lfloor\frac{\log\sqrt{m_t}}{\log 2}\rfloor$$

group operations and $2\lceil\sqrt{m_t}\rceil + 1$ bit operation by the above, since $g^{m'}$ has order m_t. For the third step, by repeated squaring, since $a \leq m_t$, we get this in $(\log m_t/\log 2) + 1$ group operations. The total for Pohlig-Hellman in one round is

$$2\lceil\sqrt{m_t}\rceil + 2\frac{\log m_t}{\log 2} + 1$$

group operations and $t + 2\sqrt{m_t}$ bit operations. Note that we do not need to repeat the first step if we store the multiplicands $m_1, m_1m_2, \ldots, m_1m_2\ldots m_{t-1}$.

Therefore repeating on this input, we get a total of $2\sum_i \sqrt{m_i} = O(\max_i \sqrt{m_i})$ bit operations, and no more than

$$\left(2\sum_{i=1}^{t}\lceil\sqrt{m_i}\rceil\right) + 2\frac{\log m}{\log 2} + t = O(\max_i \sqrt{m_i})$$

group operations.

Problem B5*. *Let the* Hamming weight

$$W : \mathbb{F}_{256}[Y]/(Y^4+1) \to \{0,1,2,3,4\}$$

be as defined in class; that is, if

$$a = \textstyle\sum_{i=0}^{3} a_i Y^i \in \mathbb{F}_{256}[Y]/(Y^4+1),$$

with $a_i \in \mathbb{F}_{256}$*, then*

$$W(a) = \#\{i : a_i \neq 0\}.$$

(a) *Let* $c \in \mathbb{F}_{256}[Y]/(Y^4+1)$ *be such that the map*

$$M : \mathbb{F}_{256}[Y]/(Y^4+1) \to \mathbb{F}_{256}[Y]/(Y^4+1)$$

defined by $M(a) = c \cdot a$ *satisfies* $M = M^{-1}$*. Prove that there exists* $a \in \mathbb{F}_{256}[Y]/(Y^4+1)$*,* $a \neq 0$*, such that* $W(a) + W(M(a)) < 5$*. [Note: if you use the theorem stated about this in class, prove it.]*

(b) *Discuss the implications of the result of* (a) *for the design of Rijndael.*

Solution. The condition (a) says that M^2 acts as the identity, i.e. $c^2 \equiv 1 \pmod{Y^4+1}$. That implies that if $c = c_0 + c_1Y + c_2Y^2 + c_3Y^3$ then

$$c_0^2 + c_1^2Y^2 + c_2Y^4 + c_3Y^6 \equiv (c_0^2 + c_2^2) + (c_1^2 + c_3^2)Y^2 \pmod{Y^4+1}.$$

Therefore $(c_0 + c_2)^2 = 1$, so $c_2 = c_0 + 1$, and $(c_1 + c_3)^2 = 0$, so $c_3 = c_1$. Therefore c is of the form $c = c_0 + c_1Y + (c_0+1)Y^2 + c_1Y^3$.

(Note that this fails our theorem from class, because the coefficients $c_3/c_1 = 1 = c_1/c_3$ are equal. We will not use this, though.)

We find $W(a) + W(M(a)) \leq 4$. It is enough to look for $W(a) = 2$ such that $M(a) = a$. This is like a previous homework problem: we could do it via equations

(which is a bit tiresome!), but rather, we represent the matrix $M : \mathbb{F}_{256}^4 \to \mathbb{F}_{256}^4$ on the basis

$$1 = (1,0,0,0), Y = (0,1,0,0), Y^2 = (0,0,1,0), Y^3 = (0,0,0,1)$$

as

$$M = \begin{pmatrix} c_0 & c_3 & c_2 & c_1 \\ c_1 & c_0 & c_3 & c_2 \\ c_2 & c_1 & c_0 & c_3 \\ c_3 & c_2 & c_1 & c_0 \end{pmatrix}$$

since, for instance,

$$M(1,0,0,0)^t = (c_0, c_1, c_2, c_3) = c = c \cdot 1.$$

Now recall that $c_3 = c_1$ and $c_2 = c_0 + 1$. We look for an element fixed by this matrix, which is the eigenspace corresponding to the eigenvalue 1. We want to find the nullspace of

$$M - I = M + I = \begin{pmatrix} c_0+1 & c_1 & c_0+1 & c_1 \\ c_1 & c_0+1 & c_1 & c_0+1 \\ c_0+1 & c_1 & c_0+1 & c_1 \\ c_1 & c_0+1 & c_1 & c_0+1 \end{pmatrix}$$

which is row equivalent to

$$\begin{pmatrix} c_0+1 & c_1 & c_0+1 & c_1 \\ c_1 & c_0+1 & c_1 & c_0+1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

and then by adding the second row to the first, we obtain (assuming $c_0+c_1+1 \neq 0$)

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ c_0+1 & c_1 & c_0+1 & c_1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

which simplifies to

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

This gives the eigenspace (a_0, a_1, a_0, a_1). For example, $1 + Y^2 = (1,0,1,0)$ is such an element, and we verify

$$(c_0 + c_1 Y + (c_0+1)Y^2 + c_1 Y^3)(1 + Y^2) = 1 + Y^2.$$

The implication for Rijndael is that a choice of c such that $c^2 \equiv 1 \pmod{Y^4+1}$ has reduced security: the diffusion requirement for a cryptosystem requires that

$$d(w, w') + d(M(w), M(w')) \geq 5.$$

Equivalently, for all $v = w + w' \neq 0$, we insist that

$$W(w+w')+W(M(w)+M(w')) = W(w+w')+W(M(w+w')) = W(v)+W(M(v)) \geq 5.$$

Such a choice for M fails this condition.

Problem B6*.

(a) *Let r be a prime number, and let n be a positive integer for which $(\mathbb{Z}/n\mathbb{Z})^*$ has an element of order r. Prove: n is divisible by r or by a prime number that is $1 \pmod r$.*

(b) *Use* (a) *to prove the following theorem, which was stated without proof in class:*

> **Theorem.** *Let r be a prime number, and let k be an integer satisfying $0 < k \leq r$. Then the number $kr + 1$ is a prime number if and only if there exists an integer a satisfying $a^k \equiv 1 \pmod{kr+1}$ and $a^{kr} \equiv 1 \pmod{kr+1}$.*

Solution. Recall that $(\mathbb{Z}/n\mathbb{Z})^*$ has order $\phi(n)$, where

$$\phi(n) = \prod_{p^e \| n} p^{e-1}(p-1)$$

which is to say that if $n = p_1^{e_1} \dots p_t^{e_t}$, then

$$\phi(n) = p_1^{e_1-1}(p_1-1) \dots p_t^{e_t-1}(p_t-1).$$

In particular, $(\mathbb{Z}/n\mathbb{Z})^*$ is a group, so if it has an element of order r, then $r \mid \phi(n)$. Since r is prime, this implies that $r = p_i$ for some i, so then $r \mid n$, or $r \mid p_i - 1$ for some i, hence $p_i \equiv 1 \pmod r$, which is the second case. This proves the claim in (a).

For (b), we note that the element a^k has order r. Since $(a^k)^r = a^{kr} \equiv 1 \pmod n$ by assumption, the order of a^k divides r; but this is prime, so since $a^k \not\equiv 1 \pmod n$, a^k cannot have order 1 so it has order r. By part (a), since $r \nmid n = kr + 1$, this implies that $n = kr + 1$ is divisible by a prime number which is $1 \pmod r$. In particular, $p > r$. Therefore $p = ar + 1$ for some positive integer a, but p divides $n = kr + 1$, so $bp = kr + 1$. Multiplying the first by b and subtracting we obtain

$$b - 1 = (k - ab)r$$

so $b \equiv 1 \pmod r$. Therefore $b = 1$, and $p = kr + 1 = n$ is prime, or $b > r$, so $kr + 1 > pr$, which since $p > r$ implies $k > r$, a contradiction.

Problem B7*. *Let $f \in \mathbb{F}_7[X]$ be a cubic polynomial with nonzero discriminant, and let the elliptic curves E_1 and E_2 over $\mathbb{F}_7$ be defined by*

$$E_1 : y^2 = f(x), \quad E_2 : y^2 = -f(x).$$

(a) *Prove: $\#E_1(\mathbb{F}_7) + \#E_2(\mathbb{F}_7) = 16$.*

(b) *Let $f = X^3 + 4$. Compute $\#E_1(\mathbb{F}_7)$.*

(c) *Construct an elliptic curve E over $\mathbb{F}_7$ such that $E(\mathbb{F}_7)$ has a point of order 13.*

Solution. First, note that -1 is not a square in $\mathbb{F}_7$. You can check this directly by squaring all of the elements. (Another way: $\#\mathbb{F}_7^* = 6$, so there is no element of order 4 in this multiplicative group: a squareroot of -1 would give such an element, which is impossible.)

For each $x \in \mathbb{F}_7$, consider the value $f(x)$. If $f(x) = 0$, then we have $(x, 0)$ as a point on *both* curves. If $f(x)$ is a square, then we have the two points $(x, \pm y)$ on E_1 for such a squareroot y. Otherwise, $-f(x)$ must be a square. One can check this directly by listing the possibilities in a table, for example, 3 is not a square

but $-3 = 4 = 2^2$ is, -1 is not a square but $-(-1) = 1$ is. Therefore we obtain two (distinct) points on E_2. Since for each of the 7 values of x we get 2 points on one or both curves, we get a total of 14; together with the points at infinity, they total to 16.

For (b), we compute that $E_1(\mathbb{F}_7) = \{(0, \pm 2)\} \cup \{O\}$. We see that $x = 0$ gives $y^2 = 4$, so $y = \pm 2$, and for all other valuse $x = 1, 2, \ldots, 6$, we obtain $f(x) = 3$ or $f(x) = 5$, which are not squares. Therefore $\#E_1(\mathbb{F}_7) = 3$.

Therefore $E_2 : y^2 = -X^3 - 4$ is an elliptic curve with $\#E_2 = 13$. Since any group of prime order is cyclic, any non-identity element is a point of order 13.

Problem B8*. *This is an open-ended problem on Mersenne primes. A* Mersenne number *is a number of the form* $2^p - 1$ *where* p *is a prime number, and a* Mersenne prime *is a Mersenne number that is prime.*

Investigate what is known about Mersenne primes. In particular: how does one test whether a given Mersenne number is prime? what is the complexity of this method? which are the known Mersenne primes? You may also cover other issues if you like, such as the connection between Mersenne numbers and perfect *numbers.*

Express what you find in your own words, and do not turn in more than three pages.

Solution. Many answers to this are possible. A clearinghouse for information on Mersenne primes is available at the Great Internet Mersenne Prime Search (GIMPS) Home Page:

`http://www.mersenne.org/prime.htm`.