Math 124: Final Examination Solutions

William Stein

Math 124 Harvard University **Fall 2001**

1. **First proof (using induction):** The statement is true when $n = 1$, since $\gcd(1,1) = 1$. Now assume that $n \geq 2$ is an integer such that $\gcd(F_{n-1}, F_n) = 1$. If there is a prime p such that
$$p \mid \gcd(F_n, F_{n+1}) = \gcd(F_n, F_n + F_{n-1}),$$
then $p \mid F_n$ and $p \mid F_n + F_{n-1}$, so $p \mid F_{n-1}$ and $p \mid F_n$, hence $p \mid \gcd(F_{n-1}, F_n)$ which contradicts our inductive assumption. Thus no such prime p exists, and $\gcd(F_n, F_{n+1}) = 1$.

   Second proof (using continued fractions): Consider the periodic continued fraction $[1, 1, 1, ...]$. The nth convergent to this continued fraction is p_n/q_n, where p_n and q_n are defined by the recurrence $p_n = p_{n-1} + p_{n-2}$, $q_n = q_{n-1} + q_{n-2}$, and $p_{-1} = p_0 = 1$, $q_{-1} = 0$, $q_0 = 1$. As observed in Lecture 17, $\gcd(p_n, q_n) = 1$. Now just notice that $p_n = F_{n+2}$ and $q_n = F_{n+1}$.

2. We do part (ii), which implies part (i). Let T be the set of elements in $(\mathbb{Z}/n\mathbb{Z})^*$ of order dividing 2, and let S be the complement of T in $(\mathbb{Z}/n\mathbb{Z})^*$, so
$$f(n) = \prod_{x \in S} x \cdot \prod_{x \in T} x.$$
If $x \in S$ then x^{-1} also lies in S and $x^{-1} \neq x$, so $\prod_{x \in S} x = 1$, and $f(n) = \prod_{x \in T} x$, where T is the subgroup of elements of order dividing 2. Using the Chinese Remainder Theorem, write
$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{n_1}\mathbb{Z})^* \times \cdots (\mathbb{Z}/p_r^{n_r}\mathbb{Z})^*,$$
where $n = \prod p_i^{n_i}$ is the prime factorization of n. Since each p_i is odd, problem 4 of this exam implies that $(\mathbb{Z}/p_i^{n_i}\mathbb{Z})^*$ is cyclic, so -1 is the only element it contains of order 2.

   Thus the group T is isomorphic to the $\mathbb{F} = (\mathbb{Z}/2\mathbb{Z})$-vector space $\mathbb{F}^r$, where again r is the number of prime factors of n. By a careful induction we see that $\sum_{a \in \mathbb{F}^r} \neq 0$ if and only if $r = 1$. To see this, check the cases $r = 0, 1, 2$ directly. For $r \geq 3$, write $\mathbb{F}^r$ as a union of two $(r-1)$-dimensional hyperplanes, the elements of each of which sum to 0, by the inductive hypothesis. Thus
$$f(n) = \begin{cases} -1, & \text{when } n \neq 1 \text{ is a prime power} \\ 1, & \text{otherwise} \end{cases}$$
   For fun, here is a PARI program that compute $f(n)$ directly, so you can verify computationally that the above result is plausible:

```
f(n)=local(s);s=1;for(x=1,n,if(gcd(x,n)==1,s=(s*x)%n));return(s);
```

3. (i) $m^e = 267882027458254785570095246784538$

(ii) The decryption key is the inverse of e modulo $\varphi(n)$, which is

$$d = 20883063260730643163672437144610 3.$$

(iii) 2002.

4. First note, as observed in Lecture 6, that the group $G = (\mathbb{Z}/p^n\mathbb{Z})^*$ has order

$$\varphi(p^n) = p^n - p^{n-1} = (p-1)p^{n-1}.$$

We will prove that G is cyclic by proving that G contains an element of order $(p-1)p^{n-1}$, and we'll do this by showing that G contains an element of order $p-1$ and one of order p^{n-1}.

In Lecture 11, we proved that the group $(\mathbb{Z}/p\mathbb{Z})^*$ of order $p-1$ is cyclic, so since the homomorphism $(\mathbb{Z}/p^n\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ is surjective, there is an $x \in (\mathbb{Z}/p^n\mathbb{Z})^*$ of order a multiple of $p-1$. Then $a = x^{p^{n-1}}$ has order $p-1$. Next, letting $b = 1+p$, the binomial theorem implies that

$$\begin{aligned} b^{p^{n-2}} &= 1 + \binom{p^{n-2}}{1}p + \binom{p^{n-2}}{2}p^2 + \cdots \\ &= 1 + p^{n-1} + \frac{p^{n-2}(p^{n-2}-1)}{2}p^2 + \cdots, \end{aligned}$$

so, since $p \neq 2$, we have $b^{p^{n-2}} \not\equiv 1 \pmod{p^n}$. (This argument fails when $p = 2$; e.g., if $p = 2$ and $n = 3$, then the right-most binomial coefficient is not divisible by p^3.) Since $b^{p^{n-1}} \equiv 1 \pmod{p^n}$, we see that b has order p^{n-1}. Thus $a \cdot b$ has order $\operatorname{lcm}(p-1, p^{n-1}) = \varphi(p^n)$, which proves that $(\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic.

[If you're worried about that binomial expansion, the following remark by "A. Student" might prove helpful: For $i > 1$ we have $p^{n-i} | \binom{p^n}{i}$, because $\binom{p^n}{i} = p^n \cdot (p^n-1)\cdots(p^n-i+1)/(i!)$ and the power of p in the factorization of $i!$ satisfies $i/p + i/p^2 + \cdots \leq i(1/(p-1)) < i$.]

5. (i) Let $\alpha = [0, \overline{1, 4}]$. Then

$$\alpha = \frac{1}{1 + \frac{1}{4+\alpha}},$$

so $\alpha = (4+\alpha)/(5+\alpha)$, hence $\alpha^2 + 4\alpha - 4 = 0$, and $\alpha = -2 + 2\sqrt{2}$. Thus $[3, \overline{1, 4}] = 3 + (-2+2\sqrt{2}) = 1 + 2\sqrt{2}$. As a check, type `contfrac(1+2*sqrt(2))` into PARI.

(ii) Using PARI we quickly see that $(1+\sqrt{23})/5$ should equal $[\overline{1, 6, 3, 1}]$. To *prove* this, we have to do the algebra as in part (i). We have

$$\alpha = [\overline{1, 6, 3, 1}] = 1 + \frac{1}{6 + \frac{1}{3 + \frac{1}{1 + \frac{1}{\alpha}}}}.$$

Using basic algebra, this simplifies to

$$\alpha = \frac{22 + 29\alpha}{19 + 25\alpha}.$$

Thus

$$25\alpha^2 - 10\alpha - 22 = 0,$$

so, since $\alpha > 0$,

$$\alpha = \frac{10 + \sqrt{100 + 4 \cdot 22 \cdot 25}}{50} = \frac{1}{5}(1 + \sqrt{23}),$$

as required.

6. If m were small, this problem would be completely trivial to solve using a simple PARI command like

```
ss(n) = for(x=1,floor(sqrt(n)),if(issquare(n-x^2),print(x)))
```

However, `ss(m)` will take an extraordinarily long time to terminate, so instead we use the proof that integers of a certain form are a sum of two squares. First, factor m using, e.g., the PARI command `factor`:

$$m = 171255509 \cdot 758572081 \cdot 817611037.$$

Each of these three prime divisors is congruent to 1 modulo 4, so each is a sum of two squares. The following representations were found using the PARI command `ss` above:

$$\begin{aligned} 171255509 &= 4153^2 + 12410^2 \\ 758572081 &= 14460^2 + 23441^2 \\ 817611037 &= 17946^2 + 22261^2 \end{aligned}$$

Now we use the formula (from Lecture 21) for expressing a product of two sums of two squares as a sum of two squares

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1x_2 + y_1y_2)^2 + (x_1y_2 - x_2y_1)^2,$$

which comes from multiplication in the Gaussian integers:

```
? (4153+12410*I)*(14460+23441*I)*(17946+22261*I)
%14 = -10304665980833 - 171525258172*I
```

Thus

$$106215561890727905176155473 = 10304665980833^2 + 171525258172^2.$$

7. First, load the file `forms.gp` from Lecture 24. The command `reducedforms` computes a list of reduced forms of discriminant -888:

```
? r=reducedforms(-888)
%2 = [[1, 0, 222], [11, -6, 21], [11, 6, 21], [13, -10, 19],
      [13, 10, 19], [14, -8, 17], [14, 8, 17], [2, 0, 111],
      [3, 0, 74], [6, 0, 37], [7, -6, 33], [7, 6, 33]]
```

Thus the class group has order 12. Since `composition(r[1],r[1])` is `r[1]`, the form $(1, 0, 222)$ is the identity of the group. There are exactly two isomorphism classes of abelian groups of order 12: one is represented by $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and the other by $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. To decide which is our class group, we compute the order of each element.

```
? for(n=1,12,print1(orderform(r[n],r[1]),"   "))
1   6   6   6   6   6   6   2   2   2   3   3
```

Since no element has order 4, the class group must be

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

8. (i) One way to compute the values is to use that `ellap` is $p + 1 - M_p$:

```
? e = ellinit([0,-4,0,0,16])
? forprime(p=3,30,if(p!=11,print1(p+1-ellap(e,p),", ")))
   5, 5, 10, 10, 20, 20, 25, 30,
\\ 3  5   7  13  17  19  23  29
```

(ii) In PARI, one can compute the N_n as follows:

```
? q*prod(n=1,30,(1-q^n)^2)*prod(n=1,3,(1-q^(11*n))^2)  + O(q^30)
%22 = q - 2*q^2 - q^3 + 2*q^4 + q^5 + 2*q^6 - 2*q^7 - 2*q^9 - 2*q^10
        + q^11 - 2*q^12 + 4*q^13 + 4*q^14 - q^15 - 4*q^16 - 2*q^17
        + 4*q^18 + 2*q^20 + 2*q^21 - 2*q^22 - q^23 - 4*q^25 - 8*q^26
        + 5*q^27 - 4*q^28 + O(q^30)
```

(iii) The sums are

$$4, 6, 8, 14, 18, 24, 30,$$

so we conjecture that for $p > 29$, we have $M_p + N_p = p + 1$. (Note that we are *not* required to prove this!)

9. (i) Use the `ellap` function and that $p + 1 - a_p = N_p$:

```
? forprime(p=3,30,print1(p+1-ellap(e,p),"  "))
4  4  8  12  20  16  20  24  20
```

(ii) In the above examples, $N_p = p + 1$ for $p \equiv 3 \pmod 4$, so we conjecture in general that this relation holds. We now prove this conjecture. Supposing $p \equiv 3 \pmod 4$, we must count the number of points on $y^2 = x^3 + x$ with coordinates in $\mathbb{Z}/p\mathbb{Z}$. Since $p \equiv 3 \pmod 4$, we have $\left(\frac{-1}{p}\right) = -1$, i.e., -1 is not a perfect square. Thus if $x \in \mathbb{Z}/p\mathbb{Z}$ and $x^3 + x$ is nonzero, then *exactly one* of $x^3 + x$ or $-(x^3 + x) = (-x)^3 + (-x)$ is a perfect square. Since $x^3 + x = x(x^2+1)$ and, as just noted, x^2+1 has no root in $\mathbb{Z}/p\mathbb{Z}$, the cubic is 0 only when $x = 0$. Thus the points on E are as follows: the point at infinity, the point $(0, 0)$, and points $(x, \pm y)$ where x runs through exactly half of the nonzero elements of $\mathbb{Z}/p\mathbb{Z}$. There are thus $1 + 1 + 2 \cdot (p-1)/2 = p + 1$ points on E over $\mathbb{Z}/p\mathbb{Z}$.

10. Your answer will depend on the random number seed in your version of PARI. We use the following functions from Lecture 31.

```
{ECM(N, m)= local(E);
   E = ellinit([0,0,0,random(N),1]*Mod(1,N));
   print("E: y^2 = x^3 + ",lift(E[4]),"x+1,  P=[0,1]");
   ellpow(E,[0,1]*Mod(1,N),m);  \\ this fails if and only if we win!
}
{lcmfirst(B) =
   local(L,i); L=1; for(i=2,B,L=lcm(L,i));
   return(L);
}
```

I'm going to start with `lcmfirst(10000)`, though you might have choosen something different for m.

```
? m = lcmfirst(10000);
? N = 124531325385603661726997;
? ECM(N,m)
E: y^2 = x^3 + 90450397866599611397131x+1,  P=[0,1]
  ***   impossible inverse modulo: Mod(495899, 124531325385603661726997).
```

We have thus split N:

$$N = 495899 \cdot 251122356337890703.$$

Now apply ECM to the remaining factor:

```
? ECM(N/495899,m)
E: y^2 = x^3 + 35484437310832518x+1,  P=[0,1]
  ***   impossible inverse modulo: Mod(311221384171, 251122356337890703).
```

Thus

$$N = 495899 \cdot 311221384171 \cdot 806893.$$

The first and last factors are prime, but the middle one is composite:

```
? isprime(495899,1)
%5 = 1
? isprime(311221384171,1)
%6 = 0
? isprime(806893,1)
%7 = 1
```

When we try ECM on the second factor, it fails a few times, then succeeds:

```
? ECM(311221384171,m)
E: y^2 = x^3 + 246181556758x+1,  P=[0,1]
%8 = [0]
? ECM(311221384171,m)
E: y^2 = x^3 + 163571326944x+1,  P=[0,1]
%9 = [Mod(20641240315, 311221384171), Mod(200682828122, 311221384171)]
? ECM(311221384171,m)
E: y^2 = x^3 + 255080864418x+1,  P=[0,1]
  ***   impossible inverse modulo: Mod(888161, 311221384171).
```

Thus

$$N = 495899 \cdot 888161 \cdot 350411 \cdot 806893,$$

and `isprime` reveals that these are all prime. As a lazy double check, we use the builtin factorization routine in PARI:

```
? factor(N)
%11 =
[350411 1]
[495899 1]
[806893 1]
[888161 1]
```

11. This is an extremely difficult open problem, and I have no idea how to solve it.