Chapter 7

Other Applications

In the 1980s, about the same time that elliptic curves were being introduced into cryptography, two related applications of elliptic curves were found, one to factoring and one to primality testing. These are generalizations of classical methods that worked with multiplicative groups $\mathbf{Z}_n^\times$. The main advantage of elliptic curves stems from the fact that there are many elliptic curves mod a number n, so if one elliptic curve doesn't work, another can be tried.

The problems of factorization and primality testing are related, but are very different in nature. The largest announced factorization up to the year 2007 was of an integer with 200 digits. However, it was at that time possible to prove primality of primes of several thousand digits.

It is possible to prove that a number is composite without finding a factor. One way is to show that $a^{n-1} \not\equiv 1 \pmod{n}$ for some a with $\gcd(a, n) = 1$. Fermat's little theorem says that if n is prime and $\gcd(a, n) = 1$, then $a^{n-1} \equiv 1 \pmod{n}$, so it follows that n must be composite, even though we have not produced a factor. Of course, if $a^{n-1} \equiv 1 \pmod{n}$ for several random choices of a, we might suspect that n is probably prime. But how can we actually prove n is prime? If n has only a few digits, we can divide n by each of the primes up to $\sqrt{n}$. However, if n has hundreds of digits, this method will take too long (much longer than the predicted life of the universe). In Section 7.2, we discuss efficient methods for proving primality. Similarly, suppose we have proved that a number is composite. How do we find the factors? This is a difficult computational problem. If the smallest prime factor of n has more than a few digits, then trying all prime factors up to $\sqrt{n}$ cannot work. In Section 7.1, we give a method that works well on numbers n of around 60 digits.

7.1 Factoring Using Elliptic Curves

In the mid 1980s, Hendrik Lenstra [75] gave new impetus to the study of elliptic curves by developing an efficient factoring algorithm that used elliptic

curves. It turned out to be very effective for factoring numbers of around 60 decimal digits, and, for larger numbers, finding prime factors having around 20 to 30 decimal digits.

We start with an example.

Example 7.1

We want to factor 4453. Let E be the elliptic curve $y^2 = x^3 + 10x - 2 \bmod 4453$ and let $P = (1, 3)$. Let's try to compute $3P$. First, we compute $2P$. The slope of the tangent line at P is

$$\frac{3x^2 + 10}{2y} = \frac{13}{6} \equiv 3713 \pmod{4453}.$$

We used the fact that $\gcd(6, 4453) = 1$ to find $6^{-1} \equiv 3711 \pmod{4453}$. Using this slope, we find that $2P = (x, y)$, with

$$x \equiv 3713^2 - 2 \equiv 4332, \quad y \equiv -3713(x - 1) - 3 \equiv 3230.$$

To compute $3P$, we add P and $2P$. The slope is

$$\frac{3230 - 3}{4332 - 1} = \frac{3227}{4331}.$$

But $\gcd(4331, 4453) = 61 \neq 1$. Therefore, we cannot find $4331^{-1} \pmod{4453}$, and we cannot evaluate the slope. However, we have found the factor 61 of 4453, and therefore $4453 = 61 \cdot 73$.

Recall (Section 2.11) that

$$E(\mathbf{Z}_{4453}) = E(\mathbf{F}_{61}) \oplus E(\mathbf{F}_{73}).$$

If we look at the multiples of P mod 61 we have

$$P \equiv (1, 3),\ 2P \equiv (1, 58),\ 3P \equiv \infty,\ 4P \equiv (1, 3),\ \ldots \pmod{61}.$$

However, the multiples of P mod 73 are

$$P \equiv (1, 3),\ 2P \equiv (25, 18),\ 3P \equiv (28, 44),\ \ldots,\ 64P \equiv \infty \pmod{73}.$$

Therefore, when we computed $3P$ mod 4453, we obtained ∞ mod 61 and a finite point mod 73. This is why the slope had a 61 in the denominator and was therefore infinite mod 61. If the order of P mod 73 had been 3 instead of 64, the slope would have had 0 mod 4453 in its denominator and the gcd would have been 4453, which would have meant that we did not obtain the factorization of 4453. But the probability is low that the order of a point mod 61 is exactly the same as the order of a point mod 73, so this situation will usually not cause us much trouble. If we replace 4453 with a much larger composite number n and work with an elliptic curve mod n and a point P

on E, then the main problem we'll face is finding some integer k such that $kP = \infty$ mod one of the factors of n. In fact, we'll often not obtain such an integer k. But if we work with enough curves E, it is likely that at least one of them will allow us to find such a k. This is the key property of the elliptic curve factorization method. □

Before we say more about elliptic curves, let's look at the classical $p-1$ **factorization method**. We start with a composite integer n that we want to factor. Choose a random integer a and a large integer B. Compute

$$a_1 \equiv a^{B!} \pmod{n}, \text{ and } \gcd(a_1 - 1, n).$$

Note that we do not compute $a^{B!}$ and then reduce mod n, since that would overflow the computer. Instead, we can compute $a^{B!}$ mod n recursively by $a^{b!} \equiv \left(a^{(b-1)!}\right)^b \pmod{n}$, for $b = 2, 3, 4, \ldots, B$. Or we can write $B!$ in binary and do modular exponentiation by successive squaring.

We say that an integer m is **B-smooth** if all of the prime factors of m are less than or equal to B. For simplicity, assume $n = pq$ is the product of two large primes. Suppose that $p-1$ is B-smooth. Since $B!$ contains all of the primes up to B, it is likely that $B!$ is a multiple of $p-1$ (the main exception is when $p-1$ is divisible by the square of a prime that is between $B/2$ and B). Therefore,

$$a_1 \equiv a^{B!} \equiv 1 \pmod{p}$$

by Fermat's little theorem (we ignore the very unlikely case that $p|a$).

Now suppose $q-1$ is divisible by a prime $\ell > B$. Among all the elements in the cyclic group $\mathbf{Z}_q^\times$, there are at most $(q-1)/\ell$ that have order not divisible by ℓ and at least $(\ell-1)(q-1)/\ell$ that have order divisible by ℓ. (These numbers are exact if $\ell^2 \nmid q-1$.) Therefore, it is very likely that the order of a is divisible by ℓ, and therefore

$$a_1 \equiv a^{B!} \not\equiv 1 \pmod{q}.$$

Therefore, $a_1 - 1$ is a multiple of p but is not a multiple of q, so

$$\gcd(a_1 - 1,\, pq) = p.$$

If all the prime factors of $q-1$ are less than B, we usually obtain $\gcd(a_1 - 1, n) = n$. In this case, we can try a smaller B, or use various other procedures (similar to the one in Section 6.8). The main problem is choosing B so that $p-1$ (or $q-1$) is B-smooth. If we choose B small, the probability of this is low. If we choose B very large, then the computation of a_1 becomes too lengthy. So we need to choose B of medium size, maybe around 10^8. But what if both $p-1$ and $q-1$ have prime factors of around 20 decimal digits? We could keep trying various random choices of a, hoping to get lucky. But the above calculation shows that if there is a prime ℓ' with $\ell' | p-1$ but $\ell' > B$,

then the chance that $a_1 \equiv 1 \pmod{p}$ is at most $1/\ell'$. This is very small if $\ell' \approx 10^{20}$. There seems to be no way to get the method to work. The elliptic curve method has a much better chance of success in this case because it allows us to change groups.

In the elliptic curve factorization method, we will need to choose random elliptic curves mod n and random points on these curves. A good way to do this is as follows. Choose a random integer A mod n and a random pair of integers $P = (u, v)$ mod n. Then choose C (the letter B is currently being used for the bound) such that

$$C = v^2 - u^3 - Au \pmod{n}.$$

This yields an elliptic curve $y^2 = x^3 + Ax + C$ with a point (u, v). This is much more efficient than the naive method of choosing A, C, u, then trying to find v. In fact, since being able to find square roots mod n is computationally equivalent to factoring n, this naive method will almost surely fail.

Here is the **elliptic curve factorization method**. We start with a composite integer n (assume n is odd) that we want to factor and do the following.

1. Choose several (usually around 10 to 20) random elliptic curves E_i : $y^2 = x^3 + A_i x + B_i$ and points P_i mod n.

2. Choose an integer B (perhaps around 10^8) and compute $(B!)P_i$ on E_i for each i.

3. If step 2 fails because some slope does not exist mod n, then we have found a factor of n.

4. If step 2 succeeds, increase B or choose new random curves E_i and points P_i and start over.

Steps 2, 3, 4 can often be done in parallel using all of the curves E_i simultaneously.

The elliptic curve method is very successful in finding a prime factor p of n when $p < 10^{40}$. Suppose we have a random integer n of around 100 decimal digits, and we know it is composite (perhaps, for example, $2^{n-1} \not\equiv 1 \pmod{n}$, so Fermat's little theorem implies that n is not prime). If we cannot find a small prime factor (by testing all of the primes up to 10^7, for example), then the elliptic curve method is worth trying since there is a good chance that n will have a prime factor less than 10^{40}.

Values of n that are used in cryptographic applications are now usually chosen as $n = pq$ with both p and q large (at least 75 decimal digits). For such numbers, the quadratic sieve and the number field sieve factorization methods outperform the elliptic curve method. However, the elliptic curve method is sometimes used inside these methods to look for medium sized prime factors of numbers that appear in intermediate steps.

Why does the elliptic curve method work? For simplicity, assume $n = pq$. A random elliptic curve E mod n can be regarded as an elliptic curve mod p and an elliptic curve mod q. We know, by Hasse's theorem, that

$$p + 1 - 2\sqrt{p} < \#E(\mathbf{F}_p) < p + 1 + 2\sqrt{p}.$$

In fact, each integer in the interval $(p+1-2\sqrt{p},\ p+1+2\sqrt{p})$ occurs for some elliptic curve. If B is of reasonable size, then the density of B-smooth integers in this interval is high enough, and the distribution of orders of random elliptic curves is sufficiently uniform. Therefore, if we choose several random E, at least one will probably have B-smooth order. In particular, if P lies on this E, then it is likely that $(B!)P = \infty \pmod p$ (as in the $p-1$ method, the main exception occurs when the order is divisible by the square of a prime near B). It is unlikely that the corresponding point P on E mod q will satisfy $(B!)P = \infty \pmod q$. (If it does, choose a smaller B or use the techniques of Section 6.8 to factor n.) Therefore, when computing $(B!)P \pmod n$, we expect to obtain a slope whose denominator is divisible by p but not by q. The gcd of this denominator with n yields the factor p.

In summary, the difference between the $p-1$ method and the elliptic curve method is the following. In the $p-1$ method, there is a reasonable chance that $p-1$ is B-smooth, but if it is not, there is not much we can do. In the elliptic curve method, there is a reasonable chance that $\#E(\mathbf{F}_p)$ is B-smooth, but if it is not we can choose another elliptic curve E.

It is interesting to note that the elliptic curve method, when applied to singular curves (see Section 2.10), yields classical factorization methods.

First, let's consider the curve E given by $y^2 = x^2(x+1)$ mod n. We showed in Theorem 2.31 that the map

$$(x, y) \mapsto \frac{x+y}{x-y}$$

is an isomorphism from $E_{ns} = E(\mathbf{Z}_n)\backslash(0,0)$ to $\mathbf{Z}_n^\times$. (Actually, we only showed this for fields. But it is true mod p and mod q, so the Chinese Remainder Theorem allows us to get the result mod $n = pq$.) A random point P on E_{ns} corresponds to a random $a \in \mathbf{Z}_n^\times$. Calculating $(B!)P$ corresponds to computing $a_1 \equiv a^{B!} \pmod n$. We have $(B!)P = \infty \pmod p$ if and only if $a_1 \equiv 1 \pmod p$, since ∞ and 1 are the identity elements of their respective groups. Fortunately, we have ways to extract the prime factor p of n in both cases. The first is by computing the gcd in the calculation of a slope. The second is by computing $\gcd(a_1 - 1, n)$. Therefore, we see that the elliptic curve method for the singular curve $y^2 = x^2(x+1)$ is really the $p-1$ method in disguise.

If we consider $y^2 = x^2(x+a)$ when a is not a square mod p, then we get the classical $p+1$ factoring method (see Exercise 7.2).

Now let's consider E given by $y^2 = x^3$. By Theorem 2.30, the map

$$(x, y) \mapsto \frac{x}{y}$$

is an isomorphism from $E_{ns} = E(\mathbf{Z}_n) \setminus (0,0)$ to $\mathbf{Z}_n$, regarded as an additive group. A random point P in E_{ns} corresponds to a random integer a mod n. Computing $(B!)P$ corresponds to computing $(B!)a \pmod{n}$. We have $(B!)P = \infty \pmod{p}$ if and only if $(B!)a \equiv 0 \pmod{p}$, which occurs if and only if $p \leq B$ (note that this is much less likely than having $p-1$ be B-smooth). Essentially, this reduces to the easiest factorization method: divide n by each of the primes up to B. This method is impractical if the smallest prime factor of n is not small. But at least it is almost an efficient way to do it. If we replace $B!$ by the product Q of primes up to B, then computing $\gcd(Q, n)$ is often faster than trying each prime separately.

7.2 Primality Testing

Suppose n is an integer of several hundred decimal digits. It is usually easy to decide with reasonable certainty whether n is prime or composite. But suppose we actually want to prove that our answer is correct. If n is composite, then usually either we know a nontrivial factor (so the proof that n is composite consists of giving the factor) or n failed a pseudoprimality test (for example, perhaps $a^{n-1} \not\equiv 1 \pmod{n}$ for some a). Therefore, when n is composite, it is usually easy to prove it, and the proof can be stated in a form that can be checked easily. But if n is prime, the situation is more difficult. Saying that n passed several pseudoprimality tests indicates that n is probably prime, but does not prove that n is prime. Saying that a computer checked all primes up to $\sqrt{n}$ is not very satisfying (and is not believable when n has several hundred digits). Cohen and Lenstra developed methods involving Jacobi sums that work well for primes of a few hundred digits. However, for primes of a thousand digits or more, the most popular method currently in use involves elliptic curves. (*Note*: For primes restricted to special classes, such as Mersenne primes, there are special methods. However, we are considering randomly chosen primes.)

The elliptic curve primality test is an elliptic curve version of the classical **Pocklington-Lehmer primality test**. Let's look at it first.

PROPOSITION 7.1

Let $n > 1$ be an integer, and let $n - 1 = rs$ with $r \geq \sqrt{n}$. Suppose that, for each prime $\ell | r$, there exists an integer a_ℓ with

$$a_\ell^{n-1} \equiv 1 \pmod{n} \text{ and } \gcd\left(a_\ell^{(n-1)/\ell} - 1, n\right) = 1.$$

Then n is prime.

PROOF Let p be a prime factor of n and let ℓ^e be the highest power of ℓ dividing r. Let $b \equiv a_\ell^{(n-1)/\ell^e} \pmod{p}$. Then

$$b^{\ell^e} \equiv a_\ell^{n-1} \equiv 1 \pmod{p} \text{ and } b^{\ell^{e-1}} \equiv a_\ell^{(n-1)/\ell} \not\equiv 1 \pmod{p},$$

since $\gcd\left(a_\ell^{(n-1)/\ell} - 1, n\right) = 1$. It follows that the order of $b \pmod{p}$ is ℓ^e. Therefore, $\ell^e | p-1$. Since this is true for every prime power factor ℓ^e of r, we have $r|p-1$. In particular,

$$p > r \geq \sqrt{n}.$$

If n is composite, it must have a prime factor at most $\sqrt{n}$. We have shown this is not the case, so n is prime. ∎

REMARK 7.2 A converse of Proposition 7.1 is true. See Exercise 7.3. ∎

Example 7.2

Let $n = 153533$. Then $n - 1 = 4 \cdot 131 \cdot 293$. Let $r = 4 \cdot 131$. The primes dividing r are $\ell = 2$ and $\ell = 131$. We have

$$2^{n-1} \equiv 1 \pmod{n} \text{ and } \gcd\left(2^{(n-1)/2} - 1, n\right) = 1,$$

so we can take $a_2 = 2$. Also,

$$2^{n-1} \equiv 1 \pmod{n} \text{ and } \gcd\left(2^{(n-1)/131} - 1, n\right) = 1,$$

so we can take $a_{131} = 2$, also. The hypotheses of Proposition 7.1 are satisfied, so we have proved that 153533 is prime. The fact that $a_2 = a_{131}$ can be regarded as coincidence. In fact, we could take $a_2 = a_{131} = a_{293} = 2$, which shows that 2 is a primitive root mod 153533 (see Appendix A). So, in a sense, the calculations for the Pocklington-Lehmer test can be regarded as progress towards showing that there is a primitive root mod n (see Exercise 7.3).

Of course, to make the proof complete, we should prove that 2 and 131 are primes. We leave the case of 2 as an exercise and look at 131. We'll use the Pocklington-Lehmer test again. Write $130 = 2 \cdot 5 \cdot 13$. Let $r = 13$, so we have only one prime ℓ, namely $\ell = 13$. We have

$$2^{130} \equiv 1 \pmod{131} \text{ and } \gcd\left(2^{10} - 1, 131\right) = 1.$$

Therefore, we can take $a_{13} = 2$. The Pocklington-Lehmer test implies that 131 is prime. Of course, we need the fact that 13 is prime, but 13 is small enough to check by trying possible factors. □

We can compactly record the proof that an integer n is prime by stating the values of the prime factors ℓ of r and the corresponding integers a_ℓ. We

should also include proofs of primality of each of these primes ℓ. And we should include proofs of primality of the auxiliary primes used in the proofs for each ℓ, etc. Anyone can use this information to verify our proof. We never need to say how we found the numbers a_ℓ, nor how we factored r.

What happens if we cannot find enough factors of $n-1$ to obtain $r \geq \sqrt{n}$ such that we know all the prime factors ℓ of r? This is clearly a possibility if we are working with n of a thousand digits. As in the case of the $p-1$ factoring method in Section 7.1, an elliptic curve analogue comes to the rescue. Note that the number $n-1$ that we need to factor is the order of the group $\mathbf{Z}_n^\times$. If we can use elliptic curves, we can replace $n-1$ with a group order near n, but there will be enough choices for the elliptic curve that we can probably find a number that can be partially factored. The following is due to Goldwasser and Kilian [47]. Recall that a finite point in $E(\mathbf{Z}_n)$ is a point (x, y) with $x, y \in \mathbf{Z}_n$. This is in contrast to the points in $E(\mathbf{Z}_n)$ that are infinite mod some of the factors of n and therefore cannot be expressed using coordinates in $\mathbf{Z}_n$. See Section 2.10.

THEOREM 7.3

Let $n > 1$ and let E be an elliptic curve mod n. Suppose there exist distinct prime numbers $\ell_1, \ldots, \ell_k$ and finite points $P_i \in E(\mathbf{Z}_n)$ such that

1. *$\ell_i P_i = \infty$ for $1 \leq i \leq k$*
2. *$\prod_{i=1}^k \ell_i > \left(n^{1/4} + 1\right)^2$.*

Then n is prime.

PROOF Let p be a prime factor of n. Write $n = p^f n_1$ with $p \nmid n_1$. Then

$$E(\mathbf{Z}_n) = E(\mathbf{Z}_{p^f}) \oplus E(\mathbf{Z}_{n_1}).$$

Since P_i is a finite point in $E(\mathbf{Z}_n)$, it yields a finite point in $E(\mathbf{Z}_{p^f})$, namely $P_i \mod p^f$. We can further reduce and obtain a finite point $P_{i,p} = P_i \mod p$ in $E(\mathbf{F}_p)$. Since $\ell_i P_i = \infty \bmod n$, we have $\ell_i P_i = \infty$ mod every factor of n. In particular, $\ell_i P_{i,p} = \infty$ in $E(\mathbf{F}_p)$, which means that $P_{i,p}$ has order ℓ_i. It follows that

$$\ell_i \,|\, \#E(\mathbf{F}_p)$$

for all i, so $\#E(\mathbf{F}_p)$ is divisible by $\prod \ell_i$. Therefore,

$$\left(n^{1/4} + 1\right)^2 < \prod_{i=1}^k \ell_i \leq \#E(\mathbf{F}_p) < p + 1 + 2\sqrt{p} = \left(p^{1/2} + 1\right)^2,$$

so $p > \sqrt{n}$. Since all prime factors of n are greater than $\sqrt{n}$, it follows that n is prime. ∎

Example 7.3
Let $n = 907$. Let E be the elliptic curve $y^2 = x^3 + 10x - 2 \bmod n$. Let $\ell = 71$. Then

$$\ell > \left(907^{1/4} + 1\right)^2 \approx 42.1.$$

Let $P = (819, 784)$. Then $71P = \infty$. Theorem 7.3 implies that 907 is prime. Of course, we needed the fact that 71 is prime, which could also be proved using Theorem 7.3, or by direct calculation.

How did we find E and P? First, we looked at a few elliptic curves mod 907 until we found one whose order was divisible by a prime ℓ that was slightly larger than 42.1. (If we had chosen $\ell \approx 907$ then we wouldn't have made much progress, since we would still have needed to prove the primality of ℓ). In fact, to find the order of the curve, we started with curves where we knew a point. In the present case, E has the point $(1, 3)$. Using Baby Step, Giant Step, we found the order of $(1, 3)$ to be $923 = 13 \cdot 71$. Then we took $P = 13(1, 3)$, which has order 71. □

For large n, the hardest part of the algorithm is finding an elliptic curve E with a suitable number of points. One possibility is to choose random elliptic curves mod n and compute their orders, for example, using Schoof's algorithm, until an order is found that has a suitable prime factor ℓ. A more efficient procedure, due to Atkin and Morain (see [7]), uses the theory of complex multiplication to find suitable curves.

As in the Pocklington-Lehmer test, once a proof of primality is found, it can be recorded rather compactly. The Goldwasser-Kilian test has been used to prove the primality of numbers of more than 1000 decimal digits.

Exercises

7.1 Let E be $y^2 = x^3 - 20x + 21 \bmod 35$, and let $P = (15, -4)$.
(a) Factor 35 by trying to compute $3P$.
(b) Factor 35 by trying to compute $4P$ by doubling twice.
(c) Compute both $3P$ and $4P$ on E mod 5 and on E mod 7. Explain why the factor 5 is obtained by computing $3P$ and 7 is obtained by computing $4P$.

7.2 This exercise shows that when the elliptic curve factorization method is applied to the singular curve $y^2 = x^2(x+a)$ where a is not a square mod a prime p, then we obtain a method equivalent to the $p + 1$ factoring method [134]. We first describe a version of the $p+1$ method. Let p be an odd prime factor of the integer n that we want to factor. Let $t_0 = 2$ and choose a random integer $t_1 \bmod n$. Define t_m by the recurrence

relation $t_{m+2} = t_1 t_{m+1} - t_m$ for $m \geq 0$. Let β, γ be the two roots of $f(X) = X^2 - t_1 X + 1$ in $\mathbf{F}_{p^2}$. Assume that $t_1^2 - 4$ is not a square in $\mathbf{F}_p$, so $\beta, \gamma \notin \mathbf{F}_p$. Let $s_m = \beta^m + \gamma^m$ for $m \geq 0$.

(a) Show that $\beta^{m+2} = t_1 \beta^{m+1} - \beta^m$ for $m \geq 0$, and similarly for γ.

(b) Show that $s_{m+2} = t_1 s_{m+1} - s_m$ for all $m \geq 0$.

(c) Show that $t_m \equiv s_m \pmod{p}$ for all $m \geq 0$.

(d) Show that β^p is a root of $f(X) \pmod{p}$, and that $\beta^p \neq \beta$. Therefore, $\gamma = \beta^p$.

(e) Show that $\beta^{p+1} = 1$ and $\gamma^{p+1} = 1$.

(f) Show that $t_{p+1} - 2 \equiv 0 \pmod{p}$.

(g) Show that if $p+1 | B!$ for some bound B (so $p+1$ is B-smooth) then $\gcd(t_{B!} - 2, n)$ is a multiple of p. Since there are ways to compute $t_{B!} \bmod n$ quickly, this gives a factorization method.

We now show the relation with the elliptic curve factorization method. Consider a curve E given by $y^2 = x^2(x + a) \mod n$, where a is not a square mod p. Choose a random point P on E. To factor n by the elliptic curve method, we compute $B!P$. By Theorem 2.31, $P \mod p$ corresponds to an element $\beta = u + v\sqrt{a} \in \mathbf{F}_{p^2}$ with $u^2 - v^2 a = 1$.

(h) Show that β is a root of $X^2 - 2uX + 1$.

(i) Show that $B!P = \infty \bmod p$ if and only if $\beta^{B!} = 1$ in $\mathbf{F}_{p^2}$.

(j) Let $t_1 = 2u$ and define the sequence t_m as above. Show that $B!P = \infty \bmod p$ if and only if p divides $\gcd(t_{B!} - 2, n)$. Therefore, the elliptic curve method factors n exactly when the $p+1$ method factors n.

7.3 (a) Show that if n is prime and g is a primitive root mod n, then $a_\ell = g$ satisfies the hypotheses of Proposition 7.1 for all ℓ.

(b) Suppose we take $r = n - 1$ and $s = 1$ in Proposition 7.1, and suppose that there is some number g such that $a_\ell = g$ satisfies the conditions on a_ℓ for each ℓ. Show that g is a primitive root mod n. (*Hint:* What power of ℓ divides the order of $g \mod n$?)

7.4 The proof of Theorem 7.3 works for singular curves given by a Weierstrass equation where the cubic has a double root, as in Theorem 2.31. This yields a theorem that uses $\mathbf{Z}_n^\times$, rather than $E(\mathbf{Z}_n)$, to prove that n is prime. State Theorem 7.3 in this case in terms of $\mathbf{Z}_n^\times$. (*Remark:* The analogue of Theorem 7.3 for $\mathbf{Z}_n$ is rather trivial. The condition that P_i is a finite point becomes the condition that P_i is a number mod n such that $\gcd(P_i, n) = 1$ (that is, it is not the identity for the group law mod any prime factor of n). Therefore $\ell_i P_i = \infty$ translates to $\ell_i P_i \equiv 0 \pmod{n}$, which implies that $\ell_i \equiv 0 \pmod{n}$. Since ℓ_i is prime, we must have $n = \ell_i$. Hence n is prime.)