Lecture 30: Using Elliptic Curves to Factor, Part I

William Stein

Math 124 Harvard University **Fall 2001**

In 1987, Hendrik Lenstra published the landmark paper *Factoring Integers with Elliptic Curves*, Annals of Mathematics, **126**, 649–673, which you can download from the Math 124 web page. Lenstra's method is also described in §IV.4 of Silverman and Tate's *Rational Points on Elliptic Curves*, §VIII.5 of [Davenport], and in §10.3 of Cohen's *A Course in Computational Algebraic Number Theory.*

In this lecture and the next, I will tell you about Lenstra's clever algorithm. It shines at finding "medium sized" factors of an integer N, which these days means 10 to 20 decimal digits but probaby not 30 decimal digits. The ECM method is thus not useful for earning money by factoring RSA challenge numbers, but is essential when factoring most integers. It also has small storage requirements. Lenstra writes:

> *"It turns out that ... the elliptic curve method is one of the fastest integer factorization methods that is currently used in practice. The quadratic sieve algorithm still seems to perform better on integers that are built up from two prime numbers of the same order of magnitude; such integers are of interest in cryptography."*

Lenstra's discover of the elliptic curve method was inspired by Pollard's $(p-1)$-method. I will spend most of the rest of this lecture introducing you to it.

1 Power-Smoothness

Definition 1.1 (Power-smooth). Let B be a positive integer. A positive integer n is *B-power-smooth* if all prime powers dividing n are less than or equal to B. The *power-smoothness* of n is the largest B such that n is B-power-smooth.

The following two PARI functions compute whether or not an integer is B-power-smooth and also the power-smoothness of n.

```
{ispowersmooth(n, B) =   \\ true if and only if n is B-powersmooth
   local(F,i);
   F = factor(n);
```

```
   for(i=1,matsize(F)[1],if(F[i,1]^F[i,2]>B,return(0)));
   return(1);
}

{powersmoothness(n) =    \\ the powersmoothness of n.
   local(F,L,i);
   F = factor(n);
   L = 1;
   for(i=1,matsize(F)[1],L=max(L,F[i,1]^F[i,2]));
   return(L);
}
```

2 Pollard's $(p-1)$-Method

Let N be an integer that we wish to factor. Choose a positive integer B (usually $\leq 10^6$ in practice). The Pollard $(p-1)$-method hunts for prime divisors p of N such that $p-1$ is B-power-smooth. Here is the strategy. Suppose that $p \mid N$ and $a > 1$ is an integer that is prime to p. By Fermat's Little Theorem,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Assume that further that $p-1$ is B-power-smooth and let $m = \mathrm{lcm}(1, 2, 3, \ldots B)$. Then $B \mid m$, so $p-1 \mid m$, and so

$$a^m \equiv 1 \pmod{p}.$$

Thus

$$p \mid \gcd(a^m - 1, N) > 1.$$

Usually $\gcd(a^m - 1, N) < N$ also, and when this is the case we have split N. In the unlikely case when $\gcd(a^m - 1, N) = N$, then $a^m \equiv 1 \pmod{q^r}$ for every prime power divisor of N. In this case, repeat the above steps but with a smaller choice of B (so that m is smaller). Also, it's a good idea to check from the start whether or not N is not a perfect power M^r, and if so replace N by M.

In practice, we don't know p. We choose a B, then an a, cross our fingers, and proceed. If we split N, great! If not, increase B or change a and try again.

For fixed B, this algorithm works when N is divisible by a prime p such that $p-1$ is B-power-smooth. How many primes p have the property that $p-1$ is B-power-smooth? Is this very common or not? Using the above two functions, we find that roughly 15% of primes p between 10^{15} and $10^{15}+10000$ are such that $p-1$ is 10^6 power-smooth.

```
\\ Count the number of B-power-smooth numbers an interval.
{cnt(B)= s=0;t=0;
   for(p=10^15, 10^15+10000,
      if(isprime(p),
```

```
        t++;if(ispowersmooth(p-1,B),s++)
      )
   );
   s/t*1.0
}
? cnt(10^6)
%5 = 0.1482889733840304182509505703
```

Thus the Pollard $(p-1)$-method with $B = 10^6$ is blind to 85% of the primes around 10^{15}. There are nontrivial theorems about densities of power-smooth numbers, but I will not discuss them today.

3 Pollard's Method in Action!

We now illustrate the Pollard $(p-1)$-method through several examples.

Example 3.1. Let $N = 5917$. We try to use the Pollard $p-1$ method with $B = 5$ to split N. We have $m = \mathrm{lcm}(1, 2, 3, 4, 5) = 60$. Take $a = 2$. We have

$$2^{60} - 1 \equiv 3416 \pmod{5917}, \qquad \text{(can compute quickly!)}$$

so

$$\gcd(2^{60} - 1, 5917) = \gcd(3416, 5917) = 61.$$

Wow, we found a prime factor of N!

In PARI, these computations are carried out as follows:

```
{lcmfirst(B) =  \\ compute the lcm of 1,2,3,...,B
    local(L,i);
    L=1;
    for(i=2,B,L=lcm(L,i));
    return(L);}
? lcmfirst(5)
%8 = 60
? Mod(2,5917)^60 - 1
%9 = Mod(3416, 5917)
? gcd(3416,5917)
%10 = 61
```

Example 3.2. Let $N = 779167$. First try $B = 5$ and $a = 2$:

$$2^{60} - 1 \equiv 710980 \pmod{N},$$

and $\gcd(2^{60} - 1, N) = 1$. Thus no prime divisor p of N has the property that $p - 1$ is 5-power-smooth. Next, we try $B = 15$. We have $m = \mathrm{lcm}(1, 2, \ldots, 15) = 360360$, and

$$2^{360360} - 1 \equiv 584876 \pmod{N},$$

so

$$\gcd(2^{360360} - 1, N) = 2003,$$

and we have split N!

Example 3.3. Let $N = 61 \cdot 71$. Then both $61 - 1 = 60 = 2^2 \cdot 3 \cdot 5$ and $71 - 1 = 2 \cdot 5 \cdot 7$ are 7-power-smooth, so Pollard's $(p-1)$-method with any $B \geq 7$ will fail, but in a confidence-inspiring way. Suppose $B = 7$, so $m = \text{lcm}(1, 2, \ldots, 7) = 420$. Then

$$2^{420} - 1 \equiv 0 \pmod{N},$$

so $\gcd(2^{420} - 1, N) = N$, and we get nothing. If we shrink B to 5, then Pollard works:

$$2^{60} - 1 \equiv 1464 \pmod{N},$$

and $\gcd(2^{60} - 1, N) = 61$, so we split N.

4 Motivation for the Elliptic Curve Method

Fix an integer B. If $N = pq$ with p and q prime and neither $p - 1$ nor $q - 1$ a B-power-smooth number, then the Pollard $(p-1)$-method is extremely unlikely to work. For example, let $B = 20$ and suppose that $N = 59 \cdot 101 = 5959$. Note that neither $59 - 1 = 2 \cdot 29$ nor $107 - 1 = 2 \cdot 53$ is B-power-smooth. With $m = \text{lcm}(1, 2, 3, \ldots, 20) = 232792560$, we have

$$2^m - 1 \equiv 5944 \pmod{N},$$

and $\gcd(2^m - 1, N) = 1$, so we get nothing.

As remarked above, the problem is that $p - 1$ is not 20-power-smooth for either $p = 59$ or $p = 101$. However, notice that $p - 2 = 3 \cdot 19$ is 20-power-smooth! If we could somehow replace the group $(\mathbb{Z}/p\mathbb{Z})^*$, which has order $p - 1$, by a group of order $p - 2$, and compute a^m for an element of this *new* group, then we might easily split N. Roughly speaking, this is what Lenstra's elliptic curve factorization method does; it replaces $(\mathbb{Z}/p\mathbb{Z})^*$ by an elliptic curve E over $\mathbb{Z}/p\mathbb{Z}$. The order of the group $E(\mathbb{Z}/p\mathbb{Z})$ is $p + 1 \pm s$ for some nonnegative integer $s < 2\sqrt{p}$ (any s can occur). For example, if E is the elliptic curve

$$y^2 = x^3 + x + 54$$

over $\mathbb{Z}/59\mathbb{Z}$ then $E(\mathbb{Z}/59\mathbb{Z})$ is cyclic of order 57. The set of numbers $59 + 1 \pm s$ for $s \leq 15$ contain numbers with very small power-smoothness.

I won't describe the elliptic curve factorization method until the next lecture. The basic idea is as follows. Suppose that we wish to factor N. Choose an integer B. Choose a random point P and a random elliptic curve $y^2 = x^3 + ax + b$ "over $\mathbb{Z}/N\mathbb{Z}$" that goes through P. Let $m = \text{lcm}(1, 2, \ldots, B)$. Try to compute mP working modulo N and using the group law formulas. If at some point it is necessary to divide modulo N, but division is not possible, we (usually) find a nontrivial factor of N. Something going wrong and not being able to divide is analogous to a^m being congruent to 1 modulo p.

More details next time!