Integer Factorisation with Elliptic Curves over Finite Fields

Will Bolton

February 16, 2016

Fields and finite fields

Definition
A field is a commutative, unital ring in which every non-zero element is invertible

The group $\mathbb{Z}_n$ is a field if and only if n is prime.

The Euclidean Algorithm

Definition

The euclidean algorithm takes two numbers and returns their *greatest common divisor (gcd)* by repeated division with remainder.

$$\begin{aligned} \gcd(21,15): 21 &= 1 \times 15 + 6 \\ 15 &= 2 \times 6 + 3 \\ 6 &= 2 \times 3 + 0 \end{aligned}$$

So $\gcd(21, 15) = 3$

The Euclidean Algorithm

Using the steps of the algorithm, it is possible to calculate

$$\begin{aligned}\gcd(21, 15) = 3 &= 1 \times 15 - 2 \times 6 \\ &= 15 - 2 \times (21 - 1 \times 15) \\ &= 15 - 2 \times 21 + 2 \times 15 \\ &= 3 \times 15 - 2 \times 21\end{aligned}$$

So $3 = 3 \times 15 - 2 \times 21$

Elliptic curves and the projective plane

Definition

The projective plane is an extension of regular 2-dimensional euclidean space by adding "points at infinity" such that every pair of lines intersects exactly once.

Definition

An elliptic curve is a non-singular cubic projective curve. For our purposes, they can all be written as $y^2 = f(x)$, where $f(x)$ is a cubic polynomial in x with no repeated roots.

The elliptic curve addition law

The points on an elliptic curve can be turned into a group via the "chord-tangent law"

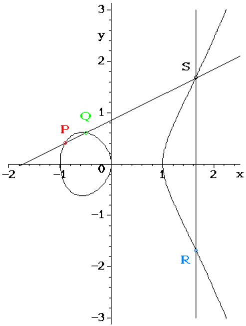

Figure : The addition law on an elliptic curve[1]

[1] Diagram taken from
http://crypto.stackexchange.com/questions/11518/what-is-so-special-about-elliptic-curves

The elliptic curve addition law

For elliptic curves over a finite field $\mathbb{F}_p$, when adding points $(x_1, y_1) + (x_2, y_2) = (x', y')$,

$$x' = \lambda^2 - a - x_1 - x_2, \quad y' = \lambda x_1 - \lambda x' - y_1$$

where $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ if $x_1 \neq x_2$ or $\lambda = \frac{3x_1^2 + 2ax_1 + b}{2y_1}$ otherwise.

Lenstra's algorithm

Definition

Lenstra's algorithm goes roughly as follows to factor an integer N:

- Choose random integers b, x and $y \mod N$
- Let $P = (x, y)$ and $c := y^2 - x^3 - bx$ such that P is a point on the curve $C : Y^2 = X^3 + bX + c \mod N$
- Compute kP for large k ($k = 10!$, for example)
- If the computation of kP is successful, increment b and restart
- Continue until one of the additions fails

Example

$$N = 3103229009940552729864$$

With $P = (3, 1)$, $k = 10!$ and $b = 39850$

$$\begin{aligned}&(2191801374392476491053, 2332211434379395076998) + \\ &\quad (406058948051076877967, 3156968592727602662096)\end{aligned}$$

is impossible, since

$$\begin{aligned}2191801374392476491053 - 406058948051076877967 = \\ 1785742426341399613086\end{aligned}$$

and $\gcd(1785742426341399613086, N) = 3992747141$
A simple division then gives $N = 3992747141 \times 791648724667$