Baby step - giant step algorithm

- Again we try to find x from b given a generator g and $b = g^x$. Let $N = [\sqrt{q-1}] + 1$.
- We make two lists:

$$
\begin{array}{lr}
\underline{\text{Baby step}} & \underline{\text{Giant step}} \\
g^0 & b \\
g^1 & bg^{-N} \\
g^2 & bg^{-2N} \\
\vdots & \vdots \\
g^{N-1} & bg^{-(N-1)N}
\end{array}
$$

- We look for a match between the two lists and if we find one, say

$$g^i = bg^{-kN} \text{ then } b = g^{i+kN}$$

and we have found x.

You can always find x

- Note $0 \leq x < q - 1 \leq N^2$ so $x = x_0 + x_1 N$ for some $x_0, x_1 \leq N$.
- This means
$$b = g^x = g^{x_0} \cdot g^{x_1 N}$$
and so
$$g^{x_0} = bg^{-x_1 N}.$$
- This algorithm takes on the order of $\sqrt{q}$ many steps.

Abelian groups

- For much of this term we have been talking about something called abelian groups without saying so.
- An abelian group is a set A together with a binary operation $+$ which is both commutative and associative. $+$ has an identity and inverses.
- Examples: $(Z, +)$, $(Q, +)$, $(R^+, \cdot)$, $(Z_n, +)$, $(F_q^*, \cdot)$ where F_q^* is the non-zero elements of F_q - the multiplicative group.
- A special case of finite abelian groups is cyclic groups; groups generated by a single element by repeatedly applying the operation. In any such group we have an analogue of the discrete log problem.

Abelian groups, cont'd

- Much of the complexity in using finite cyclic abelian groups for cryptography is in the means by which they are presented.
- For RSA, we use Z_n where n was a product of two primes and the complexity came from the difficulty in factoring n.
- For the versions of discrete log cryptosystems that we have seen, the complexity comes from the manner in which the multiplicative group of a finite field is presented.
- For the cryptographic world, it seemed that the search was on for complicatedly presented cyclic groups and what better place to look for them then in algebraic geometry.

Elliptic curves

- An algebraic curve over any field F is the solution set of some polynomial $G(x, y)$ in two variables x and y.
- This generalizes the more intuitive notion of an algebraic curve over the reals. For instance $G(x, y)$ could be $x^2 + y^2 - 1$ and then the solution set is the unit circle centred at the origin.
- This curve also makes sense over other fields like the complex numbers, the rationals and even finite fields.
- The behaviour of an algebraic curve depends to some degree on the characteristic of the field. Over a field of characteristic 2, $x^2 + y^2 = (x + y)^2$ and so "the unit circle is the union of two lines".

Elliptic curves, cont'd

- Skipping ahead quickly, cubic curves (polynomials of degree three in two variables) can be put in a canonical form as long as the characteristic of the field is not 2 or 3. That form looks like this:

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

  where a and b are in your field. Call the polynomial on the right hand side $p(x)$.
- In this form, an elliptic curve is one where $p(x)$ has no multiple roots.
- Over the reals, elliptic curves in this form come in two different flavours: p has three real roots or p has one real root.

Why do we care about elliptic curves? The group law

- Very good question!
- Because they support an abelian group structure. This takes some explaining.
- The points on the elliptic curve are the elements of the group. We only need to explain how to add them.
- The easiest case is when P and Q are two different points on the curve. Draw a line between P and Q and let R be the third point of intersection with the curve. Now reflect R in the x-axis and this is $P + Q$.

Why do we care about elliptic curves? The group law

- There are a few cases not handled by the easy case. One thing we need for our group is an identity element 0; we just formally add this point to the curve (often called the point at infinity). We need 0 in the case above when the line through P and Q does not intersect the curve. In this case, we say $P + Q = 0$. Of course $P + 0 = P$ for all P.
- If $P = Q$ then we use the (formal) tangent line to the curve at P and again, if R is the other point of intersection then we reflect R in the x-axis and this is $P + P$. Finally, if the tangent line does not intersect the curve then $P + P = 0$.
- Amazingly this defines an abelian group for any elliptic curve over any field (avoiding fields with characteristic 2 or 3 for now); the truly hard thing to prove is that $+$ is associative. All the other abelian group properties are easy.