A major computational problem is: given $N \in \mathbb{N}$ to find the prime factors of N. We discuss a method due to Pollard and then the elliptic curve method.

Pollard $p-1$ method, invented by John Pollard around 1974.

Definition 27.1. Let $n = \prod_{i=1}^{r} p_i^{e_i} \in \mathbb{N}$ and let $S \in \mathbb{N}$. Then n is **S-smooth** if all $p_i \leq S$ and n is **S-power smooth** if all $p_i^{e_i} \leq S$.

Example 27.2. $528 = 2^4 \cdot 3 \cdot 11$ is 14-smooth but is not 10-smooth or 14-power smooth.

Idea: Suppose $N = pq$ where $p-1$ is S-power smooth but $q-1$ is not S-power smooth. Then if $1 < a < N$ is randomly chosen such that $gcd(a, N) = 1$ we have $a^{S!} \equiv 1 \mod p$ and, most likely, $a^{S!} \not\equiv 1 \mod q$. Hence $\gcd(a^{S!} - 1, N)$ splits N.

Pollard $p-1$ algorithm:

Input: N
Output: A factor of N
1. Choose a suitable value for S
2. Choose a random $1 < a < N$
3. $b = a$
4. for $i = 2$ to S do
5. $\quad b = b^i \mod N$
6. Return $\gcd(b-1, N)$

Example 27.3. Let $N = 124639$ and let $S = 8$. Choose $a = 2$. One can check that

$$\gcd(a^{S!} - 1, N) = 113$$

from which one deduces that $N = 113 \cdot 1103$.
This example worked because the prime $p = 113$ satisfies $p - 1 = 2^4 \cdot 7 \mid 8!$ and so $2^{8!} \equiv 1 \mod p$ while the other prime satisfies $q - 1 = 2 \cdot 19 \cdot 29$ which is not 8-smooth.
If we had tried $S < 7$ then would expect $\gcd(b-1, N) = 1$ while if we had tried $S \geq 29$ then would expect $\gcd(b-1, N) = N$.

Exercise 27.4. Factor the following numbers using the $p-1$ method (use Gap or any other package): 1157417, 10028219737, 256505540497. How do you choose S?

Exercise 27.5. The Pollard $p-1$ only factors numbers of a special form. Write down a family of integers which are hard to factor using this method.

Elliptic Curve Factoring Method (ECM), invented by Hendrik Lenstra Jr. around 1984.

Idea: Suppose $N = pq$ and suppose one has an elliptic curve E over $\mathbb{Q}$ such that $\#E(\mathbb{F}_p)$ is S-power smooth but $\#E(\mathbb{F}_q)$ is not S-power smooth. Then for $P \in E(\mathbb{Q})$ we have $[S!]P = \infty$ in $E(\mathbb{F}_p)$ but, with most likely, $[S!]P \neq \infty$ in $E(\mathbb{F}_q)$.
For the factoring algorithm, compute $[S!]P = (x, y, z)$ using projective coordinates and reducing everything modulo N. Then $\gcd(z, N)$ should split N.

ECM algorithm:

Input: N
Output: A factor of N
1. Choose a suitable value for S
2. Choose a random elliptic curve E and a point $P \in E(\mathbb{Z}_N)$ (see Exercise)
3. $Q = P = (x_P, y_P, z_P)$
4. for $i = 2$ to S do
5. $\quad Q = [i]Q$ working mod N
6. Return $\gcd(z_Q, N)$

Exercise 27.6. How can one compute a random elliptic curve with a point $P \in E(\mathbb{Z}_N)$ when the factorisation of N is not known?

Example 27.7. Let $N = 53 \cdot 83 = 4399$. Choose $E : y^2 = x^3 + 6x - 6$ and $P = (1, 1)$.
One has $\#E(\mathbb{F}_{53}) = 60 = 2^2 \cdot 3 \cdot 5$ and $\#E(\mathbb{F}_{83}) = 102 = 2 \cdot 3 \cdot 17$.
One can check that, on $E(\mathbb{F}_{53})$, $[2]P = (5, 34)$, $[6]P = (21, 0)$ and $[24]P = \infty$. While on $E(\mathbb{F}_{83})$ we have $[2]P = (39, 77)$, $[6]P = (30, 45)$ and $[24]P = (9, 69)$.
Computing $[24]P$ projectively gives a point (x, y, z) such that $53 \mid z$ but $83 \nmid z$. Hence, $\gcd(z, N) = 53$.