Быстрое возведение числа в степень. $a^n = a^{2^{p_1}+2^{p_2}+2^{p_k}}$. $(a^n)^2 = a^{2^{p_1+1}+2^{p_2+1}+2^{p_k+1}}$. Тогда чтобы получить значение a^n можно разложить n на степени двойки, а дальше работать с ним как с вектором степеней: мы можем либо приписать в конец 0 (то есть умножить на a) или прибавить ко всем числам 1 (то есть возвести в квадрат). Можно заметить, что такими операциями получится получить любую степень за логарифмическое время.

Диофантовы уравнения. Дано уравнение $ax + by = c$. Сначала разделим все на $gcd(a, b)$, получим $a'x + b'y = c'$, где $gcd(a', b') = 1$. Тогда существует решение уравнения $a'x + b'y = 1$, которое находится расширенным алгоритмом Евклида, а дальше корни можно получить умножением на c'.

Алгоритм Евклида для поиска gcd использует то, что если $a > b$ $gcd(a, b) = d$, то $a = dx,\ b = dy,\ a - b = d(x - y), gcd(a, b) = gcd(b, a - b)$. Ну тогда можно сжать много операций вычитания подряд одним взятием остатка. Брать остаток можно не более $O(\log C)$ раз — если $a > 2b$, то b явно уменьшилось в два раза, а если $a < 2b$, то $a - b < \frac{a}{2} < b$.

Теперь рассмотрим расширенный алгоритм Евклида. Он будет возвращать решение уравнения $ax + by = 1$. Мы будем пользоваться тем, что точка останова для нашего алгоритма это $a = 1,\ b = 0$, тогда $x = 1, y = 0$. Тогда можно явно предъявить пересчет рекурсии:

$$bx + (a\ mod\ b)y = 1$$

$$bx + (a - \lfloor\frac{a}{b}\rfloor b)y = 1$$

$$ay + b(x - \lfloor\frac{a}{b}\rfloor y) = 1$$

Тогда $x' = y,\ y' = x - \lfloor\frac{a}{b}\rfloor y$.

КТО. Если у нас есть набор взаимно простых чисел, которые используются как модули, то остаток по каждому из этих модулей задает число. Иначе говоря, если взять число, меньшее чем НОК модулей, то для него существует единственное представление через вектор остатков. Понятно, что размеры множества векторов и чисел меньших НОК одинаковый, для любого числа есть представление в виде вектора. Значит нам важно только то, что для любого вектора остатков существует число, у которого именно такое представление.

Построим итеративно это число. $x \equiv r_i \pmod{m_i}$. Тогда $m_1 \cdot X - m_2 \cdot Y = r_2 - r_1$. Если разность остатков равна нулю, то это просто задает нам один общий остаток по произведению модулей, а иначе мы можем найти решение, которое, опять же, задает нам остаток по произведению двух модулей.

Факторизация числа. Число можно представить в виде произведения простых чисел, каждое из которых задано в какой-то степени.

Факторизовать одно число можно за $O(\sqrt{n})$, потому что не бывает двух простых делителей числа, больших чем $\sqrt{n}$ (иначе их произведение больше чем n). Тогда можно пройтись по первым $O(\sqrt{n})$ чисел, и делить на них основное, чтобы узнать показатель степени. Это работает за $O(\sqrt{n} + \log n) = O(\sqrt{n})$.

Решето Эратосфена. Часто нам хочется сделать предподсчет, чтобы потом быстро факторизовать числа от 1 до n. Для этого хочется запомнить для всех чисел их минимальный простой делитель. Тогда факторизовать можно будет за $O(\log n)$.

Можно, например, перебрать делители, перебрать второй множитель от 1 до $\frac{n}{x}$, и проставить соответствующие пометки в клетках, которые получатся как произведение. Это будет работать за $O(n \sum_{i=1}^{n} \frac{1}{i}) = O(n \log n)$ (очень грубая оценка, можно оценить как сумму обратных простых как $O(n \log \log n)$)

Давайте сделаем решето за линейное время. Мы хотим теперь ставить пометки для каждого числа $m = x \cdot d$ только один раз — когда x это его минимальный простой делитель. Тогда, если мы для текущего числа d поставим пометку для всех чисел m, которые получаются домножением на $x \leq min\_divisor(d)$, то x будет минимальным простым делителем m, поэтому мы каждое m рассмотрим всего 1 раз.