**Euclid’s algorithm proof**

From https://crypto.stanford.edu/pbc/notes/numbertheory/euclid.html

How do you find the greatest common divisor (gcd) of two integers a, b?

We denote the greatest common divisor of a and b by gcd(a,b), or sometimes even just (a,b). If (a,b)=1, we say a and b are *coprime*.

The obvios answer is to list all divisors a and b, and look for the greatest one they have in common. However, this requires and a and b to be factorized, and no one knows how to do this efficiently.

A few simple observations lead to a far superior method: Euclid’s algorithm, or the Euclidean algorithm. First, if d divides a and d divides b, then d divides their difference, a-b , where a is the larger of the two. But this means we’ve shrunk the original problem: now we just need to find gcd(b, a-b).

We repeat until we reach a trivial case (b, 0),

Suppose we wish to compute gcd(27, 33).

(27, 33)->(27,6)->(21,6)->(15,6)->(9,6)->(6,3)->(3,3)=3

Kā atrast divu veselu skaitļu a, b lielāko kopīgo dalītāju (gcd)?

Mēs apzīmējam a un b lielāko kopīgo dalītāju ar gcd(a,b) vai dažreiz pat tikai ar (a,b). Ja (a,b)=1, mēs sakām, ka a un b ir pirmskaitļi.

Acīmredzama atbilde ir uzskaitīt visus dalītājus a un b un meklēt lielāko, kas tiem ir kopīgs. Tomēr tas prasa un a un b sadalīt pirmreizinātājos, un neviens nezina, kā to izdarīt efektīvi.

Daži vienkārši novērojumi noved pie daudz labākas metodes: Eiklīda algoritms. Pirmkārt, ja a dalās ar d un b dalās ar d, tad starpība a-b arī dalās ar d, kur a ir lielākais no abiem skaitļiem. Bet tas nozīmē, ka esam samazinājuši sākotnējo problēmu: tagad mums vienkārši jāatrod   
gcd(b, a-b).

Mēs atkārtojam, līdz sasniedzam triviālu gadījumu (b, b),

Pieņemsim, ka mēs vēlamies aprēķināt gcd(27, 33).

(27, 33)->(27,6)-> (21,6)-> (15,6)-> (9,6)->(6,3)->(3,3)=3

Vajadzīgi seši soļi.

**Improved Euclid’s algorithm**

From https://www.quora.com/What-is-the-proof-of-Euclids-algorithm

Euclid’s algorithm proof

One recursive phase of the algorithm is reducing the problem of finding GCD(a, b) into finding GCD(b, a%b). It’s being repeated until a pair is found for which the answer is obvious (a pair (x, 0) - we then obviously know the largest common divisor is x). So all that is needed to be proven is that those two pairs (a, b) and (b, a%b) have the same GCD since that means that if the algorithm ever ends than the result will be the correct GCD of the input values - and the fact that it will end is obvious, because the sum of a + b is decreasing in every iteration.

So proving that point: if some number d is a common divisor of a and b then it also divides a%b because by definition a can be written as “a = a%b + something\*b”, so since d | a and d | “something\*b”, then d must divide a%b. So we know d is a common divisor of b and a%b. The same way if some number d divides b and a%b then it also divides a. Hence when we do a step from analysing the pair (a, b) into the pair (b, a%b) we know that any common divisor of left pair is a common divisor of right pair and vice versa i.e. the have exactly the same set of common divisors. Hence of course also the largest one of them is the same for both.

Viena algoritma rekursīvā fāze samazina GCD(a, b) atrašanas problēmu līdz GCD(b, a%b) atrašanai. Tas tiek atkārtots, līdz tiek atrasts pāris, uz kuru atbilde ir acīmredzama (pāris (x, 0) — tad mēs acīmredzami zinām, ka lielākais kopīgais dalītājs ir x). Tātad viss, kas jāpierāda, ir tas, ka šiem diviem pāriem (a, b) un (b, a%b) ir vienāds GCD, jo tas nozīmē, ka, ja algoritms kādreiz beigsies, rezultāts būs pareizais GCD - un tas, ka tas beigsies, ir acīmredzams, jo a + b summa katrā iterācijā samazinās.

Tātad, pierādīsim šo punktu: ja kāds skaitlis d ir a un b kopīgs dalītājs, tad tas arī ir a%b dalītājs, jo pēc a definīcijas var uzrakstīt, ka   
“a = a%b + kaut\_kas\*b”, tātad, tā kā a dalās ar d un “kaut\_kas\*b” arī dalās ar d, tad a%b arī ir jādalās ar d. Tātad mēs zinām, ka d ir b un a% b kopīgs dalītājs. Tāpat, ja b un a%b dalās ar kādu d, tad arī a dalās ar d. Tādējādi, veicot soli no pāra (a, b) analīzes uz pāra (b, a%b) analīzi, mēs zinām, ka jebkurš kreisā pāra kopīgs dalītājs ir labā pāra kopīgs dalītājs un otrādi, t.i., tiem ir tieši tāds pati kopīgo dalītāju kopa. Tāpēc, protams, arī lielākais no dalītājiem tiem abiem ir kopīgs abiem pāriem.

Piemērs: gcd(33,27)

gcd(33,27)->gcd(27, 6)->gcd(6,3)->gcd(3,0)=3

Vajadzīgi tikai trīs soļi.