Determining a number is composite

Fermat's test:

$a^{n-1} \pmod n$ for a random a: $a \nmid n$

$\not\equiv 1 \downarrow$

n not prime

Unfortunately there are n and a : $a^{n-1} \equiv 1 \pmod n$ and n is not prime
In that case n is a pseudo-prime and a a liar.
There are even n's not prime but where $a^{n-1} \equiv 1 \pmod n$ $\forall a \in \{1, 2, \dots n-1\}$ with $\gcd(a, n)$. Those are called Carmichael numbers.

In practice you try to determine if a number is likely prime.

Fermat's factorization

we can look at factorization via the notable product: $x^2 - y^2 = (x+y)(x-y)$

for factorizing n we can take $x^2 > n$: $(x^2 - n) = y^2$ we have to find a suitable y

in that way $n \mid (x+y)$, $n \mid (x-y)$. If they are real you have found part of the prime factorization

example

$n = 466883$, n is not prime because

$$2^{466882} \equiv 153160 \not\equiv 1 \pmod{466883}$$

since:

$\sqrt{466883} = 683.288\ldots$ we calculate $(683+K)^2 - n$ for $K = 1, 2, 3, \ldots$ until we find a square

the first one we find is $702^2 - 466883 = 492804 - 466883 = 25921 = 161^2$

so: $x = 702$, $y = 161$:

$$x+y = 702 + 161 = 863 \quad \text{and} \quad x-y = 706 - 161 = 541$$

both factors are prime numbers so: $n = 863 \cdot 541$ we are done

when we find factors not prime we can decompose them further

This method works fairly well if both prime factors are of the same order of magnitude

In that case y is very small and the search isn't long

it's $O(n^n)$ so it's slow

setaccio

Sieves methods

Instead of searching for an X and Y where $n = x^2 - y^2$ we can instead search X and Y where $n \mid x^2 - y^2$, in other words:

$$x^2 \equiv y^2 \pmod{n} : x \not\equiv y \pmod{n}$$

we do that with the following steps:

- determine a set S of small prime factors
- generate (eg. randomly) numbers x_i, square them and calculate the remainder R_i when divided by n this remainder usually is not a square.
- Select the x_i's where R_i's can be factorized into prime factors by S.
- If you have found enough R_i's there's a good chance that the product of 2 or more R_i's is a square we note $\prod_{i \in A} R_i$ is a square for a certain A
- then we find that:

$$\prod_{i \in A} x_i^2 = \left(\prod_{i \in A} x_i \right)^2 = \prod_{i \in A} R_i \pmod{n}$$

- suppose now

$$X = \prod_{i \in A} x_i \quad \text{and} \quad Y = \sqrt{\prod_{i \in A} R_i}$$

then $n \mid x^2 - y^2 = (X+Y)(X-Y)$

- with a bit of luck the factors of n will then be spread over $X+Y$ and $X-Y$ if a factor p of n is also a divisor of $X+Y$ then p will also a divisor of $\gcd(X+Y, n)$. So we calculate $\gcd(X+Y, n)$ and we find a divisor of n. We do the same with $X-Y$

example:

trying to refactor $n = 466883$

Now we look for squares modulo n that can be factorized using only factors from: $S = \{2,3,5,7\}$

we generate 1000 numbers and keep those whose remainder of the square is factorizable with S

so: $169246^2 \equiv 2700 = 2^2 \cdot 3^3 \cdot 5^2 \pmod{466883}$

$14393^2 \equiv 329280 = 2^6 \cdot 3^1 \cdot 5^1 \cdot 7^3 \pmod{466883}$

$419430^2 \equiv 10500 = 2^2 \cdot 3^1 \cdot 5^3 \cdot 7^1 \pmod{466883}$

the product of the second and third remainder is a square

$(2^6 \cdot 3 \cdot 5 \cdot 7^3)(2^2 \cdot 3 \cdot 5^3 \cdot 7) = (2^8 \cdot 3^2 \cdot 5^2 \cdot 7^4) = (2^4 \cdot 3 \cdot 5 \cdot 7^2)^2$ so:

$(14393 \cdot 419430)^2 \equiv (2^4 \cdot 3 \cdot 5 \cdot 7^2)^2 \pmod{466883}$

unfortunately: $14393 \cdot 419430 \equiv 58800 \pmod{466883}$

$2^4 \cdot 3 \cdot 5^2 \cdot 7^2 \equiv 58800 \pmod{466883}$

if we set $x = 14393 \cdot 419430 \pmod{466883}$ and $y = 2^4 \cdot 3 \cdot 5^2 \cdot 7^2 \pmod{466883}$

then indeed $n \mid x^2 - y^2$ but since also $n \mid x - y$ this returns nothing. Bad luck

Let's generate other numbers

$169246^2 \equiv 2700 = 2^2 \cdot 3^3 \cdot 5^2 \pmod{466883}$

$83036^2 \equiv 49152 = 2^{14} \cdot 3^1 \pmod{466883}$

$146390^2 \equiv 102400 = 2^{12} \cdot 5^2 \pmod{466883}$

the product of the first two remainders is a square $(2^8 \cdot 3^2 \cdot 5)^2$, so:

$(169246 \cdot 83036)^2 \equiv (2^8 \cdot 3^2 \cdot 5)^2 \pmod{466883}$

also $169246 \cdot 83036 \equiv 332556 \pmod{466883}$

$2^8 \cdot 3^2 \cdot 5 \equiv 11520 \pmod{466883}$

so set $x = 332556$, $y = 11520$

since $(x^2 - y^2) = (x+y)(x-y)$ is divisible by n the prime factors are spread over $(x+y)$ and $(x-y)$

Here $n \nmid x \pm y$ so there is p factor of $x+y$ and q factor of $x-y$

but then $\gcd(x+y, n)$ is a real divisor of n (also $x-y$). In this case:

$\gcd(x+y, n) = \gcd(344076, 466883) = 541$

$\gcd(x-y, n) = \gcd(321036, 466883) = 863$

---

we could have done it faster since when generating numbers we found that:

$146390^2 \equiv 102400 = 2^{12} \cdot 5^2$ which has a square on the right

$\Leftrightarrow 146390^2 \equiv (2^6 \cdot 5)^2 \pmod{466883}$

$x = 146390$, $y = 2^6 \cdot 5 = 320$

$\gcd(x+y, n) = 863$

$\gcd(x-y, n) = 541$