Extended Euclidean Algorithm (EEA)

Input: Integers a, b with $a \geq b > 0$.

Initialize: Construct a table with four columns so that

- the columns are labelled x, y, r and q,
- the first row in the table is $(1, 0, a, 0)$,
- the second row in the table is $(0, 1, b, 0)$.

Repeat: For $i \geq 3$,

- $q_i \leftarrow \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor$
- $\text{Row}_i \leftarrow \text{Row}_{i-2} - q_i \text{Row}_{i-1}$

Stop: When $r_i = 0$.

Output: Set $n = i - 1$. Then $\gcd(a, b) = r_n$, and $s = x_n$ and $t = y_n$ are a certificate of correctness.

9.3 Proving that the RSA Scheme Works

Now that we have seen two examples of RSA and the associated computations, we prove in the following result that the RSA scheme always works. What we mean by this is that we prove the *Claim:* $R = M$, that the plaintext message M and the decrypted message received R are identical.

Theorem 1 **(RSA Works (RSA))**

For all integers p, q, n, e, d, M, C and R, if

1. p and q are distinct primes,
2. $n = pq$,
3. e and d are positive integers such that $ed \equiv 1 \pmod{(p-1)(q-1)}$ and $1 < e, d < (p-1)(q-1)$,
4. $0 \leq M < n$,
5. $M^e \equiv C \pmod{n}$ where $0 \leq C < n$,

6. $C^d \equiv R \pmod{n}$ where $0 \leq R < n$,

then $R = M$.

Proof: Let p, q, n, e, d, M, C and R be arbitrary integers, and assume that they satisfy parts 1 – 6 of the hypothesis. Now, from parts 5 and 6 of the hypothesis, we have

$$R \equiv C^d \equiv \left(M^e\right)^d \equiv M^{ed} \pmod{n}.$$

Since p and q are distinct primes, they must be coprime. Therefore, since $n = pq$, we can apply the Splitting Modulus Theorem to obtain that

$$R \equiv M^{ed} \pmod{p}$$

and

$$R \equiv M^{ed} \pmod{q}.$$

Now, we prove that $R \equiv M \pmod{p}$, by considering the two cases $p \mid M$ and $p \nmid M$.

- **Case 1:** If $p \mid M$, then we have $M \equiv 0 \pmod{p}$, and therefore,

  $$R \equiv 0^{ed} \equiv 0 \pmod{p}.$$

  Hence in this case both R and M are congruent to 0 modulo p, giving $R \equiv M \pmod{p}$.

- **Case 2:** If $p \nmid M$, then p and M are coprime, so by Fermat's Little Theorem, we have

  $$M^{p-1} \equiv 1 \pmod{p}. \tag{9.1}$$

  From part 3 of the hypothesis and the definitions of congruence and divisibility, there exists an integer k such that

  $$ed = 1 + k(p-1)(q-1).$$

  Moreover, since $ed > 1$ and $p-1$ and $q-1$ are positive integers, it must be the case that k is a positive integer. Putting these together, we obtain

  $$R \equiv M^{1+k(p-1)(q-1)} \pmod{n},$$

  for some positive integer k.

  Substituting (9.1) gives

  $$R \equiv M\left(M^{p-1}\right)^{k(q-1)} \equiv M(1)^{k(q-1)} \equiv M \pmod{p},$$

  and hence in this case we also have $R \equiv M \pmod{p}$.

Example 1 Carry out the following calculations for the RSA scheme with $p = 5$, $q = 11$ and $e = 3$.

1. Determine the private key (d, n).

   Solution: In this case, $n = 5 \times 11 = 55$ and $(p-1)(q-1) = 4 \times 10 = 40$. To find d, we solve

   $$3d \equiv 1 \pmod{40}.$$

   To do so, we set up the Linear Diophantine Equation

   $$40x + 3d = 1$$

   and use the Extended Euclidean Algorithm

x	d	r	q
1	0	40	0
0	1	3	0
1	-13	1	13
-3	40	0	3

   Hence our solution for d is

   $$d \equiv -13 \pmod{40}.$$

   Since d must satisfy $1 < d < 40$, we obtain $d = 40 - 13 = 27$, so the private key is the pair $(d, n) = (27, 55)$.

2. Suppose Bob receives the ciphertext $C = 47$. Decrypt C to determine the message M that was encrypted by Alice.

   Solution: We wish to compute $R = 47^{27} \pmod{55}$. To simplify this computation, note that 5 and 11 are coprime, so by the Splitting Modulus Theorem, we can obtain R as the unique solution to the simultaneous congruences

   $$\begin{aligned} & R \equiv 47^{27} \pmod{5} \\ \text{and} \quad & R \equiv 47^{27} \pmod{11}. \end{aligned}$$

   Now $47 \equiv 2 \pmod{5}$ and $47 \equiv 3 \pmod{11}$, therefore we have $R \equiv 2^{27} \pmod{5}$ and $R \equiv 3^{27} \pmod{11}$. Since 5 and 11 are both prime numbers, we can apply Fermat's

Little Theorem (FℓT), which gives $2^4 \equiv 1 \pmod 5$ and $3^{10} \equiv 1 \pmod{11}$. Hence, from $27 = (6)(4) + 3$, we obtain

$$R \equiv 2^{27} \equiv (2^4)^6 2^3 \equiv (1)^6 2^3 \equiv 2^3 \equiv 8 \equiv 3 \pmod 5.$$

Similarly, from $27 = 2(10) + 7$, we obtain

$$R \equiv 3^{27} \equiv (3^{10})^2 (3)^7 \equiv (1)^2 3^7 \equiv 3^7 \equiv (9)^3 3 \equiv (-2)^3 3 \equiv 9 \pmod{11}.$$

Therefore, we have to solve the simultaneous congruences

$$\begin{aligned} R &\equiv 3 \pmod 5 \\ \text{and} \quad R &\equiv 9 \pmod{11}. \end{aligned}$$

Again note that 5 and 11 are coprime, and that these simultaneous congruences are linear, so by the Chinese Remainder Theorem, there is a unique solution modulo $5 \times 11 = 55$. To shorten our work, a quick check shows that $53 \equiv 3 \pmod 5$ and $53 \equiv 9 \pmod{11}$, and so the unique solution to these simultaneous congruences is given by $R \equiv 53 \pmod{55}$. Hence we have $M = 53$.

(Congruence Add and Multiply (CAM))

For all positive integers n, for all integers $a_1, \ldots, a_n$, and $b_1, \ldots, b_n$, if $a_i \equiv b_i \pmod m$ for all $1 \leq i \leq n$, then

1. $a_1 + a_2 + \cdots + a_n \equiv b_1 + b_2 + \cdots + b_n \pmod m$,
2. $a_1 a_2 \cdots a_n \equiv b_1 b_2 \cdots b_n \pmod m$.

(Congruence Power (CP))

For all positive integers n and integers a and b, if $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$.

(Fermat's Little Theorem (FℓT))

For all prime numbers p and integers a not divisible by p, we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

What is the remainder when 3167^{2531} is divided by 17?

Solution: Observe that

$$3167 \equiv 5 \pmod{17}.$$

Also, since $17 \nmid 5$, by Fermat's Little Theorem we have

$$5^{16} \equiv 1 \pmod{17}.$$

Then, using propositions Congruence Add and Multiply, and Congruence Power, we obtain

$$3167^{2531} \equiv 5^{2531} \equiv 5^{16\cdot 158+3} \equiv (5^{16})^{158}(5^3) \equiv (1)^{158}(125) \equiv 6 \pmod{17}.$$

Since $0 \leq 6 < 17$, we conclude from the proposition Congruent To Remainder that the remainder is equal to 6.

(Chinese Remainder Theorem (CRT))

For all integers a_1 and a_2, and positive integers m_1 and m_2, if $\gcd(m_1, m_2) = 1$, then the simultaneous linear congruences

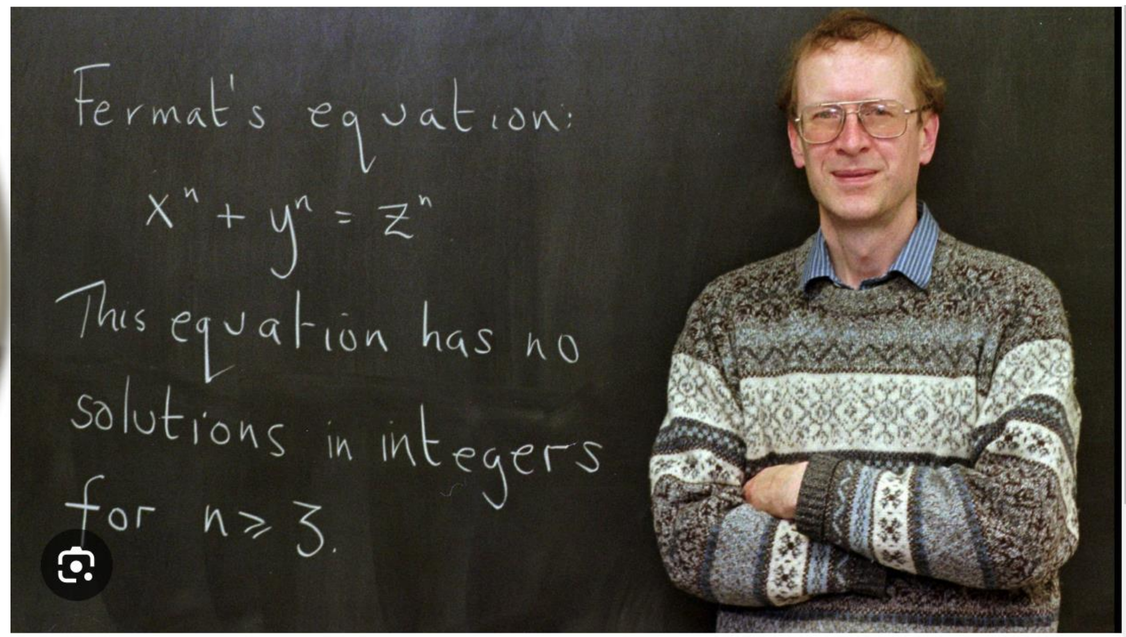
$$n \equiv a_1 \pmod{m_1}$$
$$n \equiv a_2 \pmod{m_2}$$

(Prime Factorization (PF))

Every natural number $n > 1$ can be written as a product of primes.

- **Sum of two squares theorem.** Let $n \in N$. Then there exist $a, b \in Z$ such that $n = a^2 + b^2$ if and only if the prime decomposition of n contains no factor p^k where p has remainder 3 upon division by 4 and k is odd.
- **Fermat's sum of two squares.** For an odd prime p, there exist integers x, y satisfying $p = x^2 + y^2$ if and only if reminder of p when divided by 4 is 1.

Pierre de Fermat
(1601-1665)



Andrew Wiles

Theorem: **There are infinitely many primes.**

Physicist:

In fact, every odd number is prime:

3 is prime, 5 is prime, 7 is prime, 9 is experimental error, 11 is prime, 13 is prime, 15 is experimental error, 17 is prime, 19 is prime…

The empirical evidence is overwhelming!

Euclid's Elements

Book IX

Proposition 20

Prime numbers are more than any assigned multitude of prime numbers.

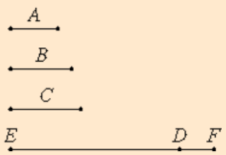
Let *A, B,* and *C* be the assigned prime numbers.

I say that there are more prime numbers than *A, B,* and *C.*

Take the least number *DE* measured by *A, B,* and *C.* Add the unit *DF* to *DE.*

Then *EF* is either prime or not.

First, let it be prime. Then the prime numbers *A, B, C,* and *EF* have been found which are more than *A, B,* and *C.*



Next, let *EF* not be prime. Therefore it is measured by some prime number. Let it be measured by the prime number *G.* VII.31

I say that *G* is not the same with any of the numbers *A, B,* and *C.*

If possible, let it be so. Now *A, B,* and *C* measure *DE,* therefore *G* also measures *DE.* But it also measures *EF.* Therefore *G,* being a number, measures the remainder, the unit *DF,* which is absurd.

Therefore *G* is not the same with any one of the numbers *A, B,* and *C.* And by hypothesis it is prime. Therefore the prime numbers *A, B, C,* and *G* have been found which are more than the assigned multitude of *A, B,* and *C.*

Therefore, *prime numbers are more than any assigned multitude of prime numbers.*

Q.E.D.

Question: Are there infinitely many primes of the form $n^2 + 1$*?*

- $\sum_{k=1}^{\infty} \frac{1}{2^k} < \infty$
- $\sum_{k=1}^{\infty} \frac{1}{k^2} < \infty$
- *Question: Is there always a prime between n^2 and $(n+1)^2$?*
- $\sum_{p\ prime}^{\infty} \frac{1}{p} > \ \infty$

- **Prime number theorem:** Number $\pi(n)$ of primes less than n satisfies $\lim_{n \to \infty} \frac{\pi(n)}{n/\log(n)} \to 1$

- Riemann Zeta function: $$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}$$

-     

-*Psychology of Invention in the Mathematical Field*, Jacques Hadamard

https://rationalwiki.org/wiki/Fun:Proof_that_all_odd_numbers_are_prime
http://aleph0.clarku.edu/~djoyce/elements/aboutText.html

More questions:

- The Odd Goldbach Problem: Every odd n > 5 is the sum of three primes.
- Goldbach's Conjecture: Every even n > 2 is the sum of two primes.
- Every even number is the difference of two primes.
- For every even number $2n$ are there infinitely many pairs of consecutive primes which differ by $2n$.