Maths for Computer Science
Divisibility and prime numbers

Denis TRYSTRAM
Lecture notes MoSIG1

oct. 2021

Motivation

A preliminary question

every even number can be written as a sum of two primes.

Motivation

A preliminary question

every even number can be written as a sum of two primes.

- Number Theory is a field where the problems to solve are very easy to formalize and to understand, but very hard to prove!
- The underlying techniques of number theory are very important in many problems, including cryptography, analysis of algorithms, etc..

The objective of this lecture is to investigate classical results and some related properties.

Some well-known examples

- Goldbach conjecture
  see previous slide
- Perfect numbers conjecture:
  is there any odd perfect number?[1]
- Twin primes:
  are there an infinite number of primes in the form $(n, n+2)$?
- etc.

[1] Perfect numbers are those which are equal to the sum of their decomposition factors (for instance $28 = 1 + 2 + 4 + 7 + 14$).

Basic results and definitions

Definition.
Let a and b be two integers.
a divides b if there is an integer k such that $ak = b$.

We also say that b is a multiple of a (notice here that a may be negative).

Remark that according to this definition, every number divides 0.

Properties

The following properties are straightforward by applying directly the definitions:

1. If $a \mid b$ then $a \mid bc$ $\forall$ integers c
2. If $a \mid b$ and $b \mid c$ then $a \mid c$
3. If $a \mid b$ and $a \mid b + c$ then $a \mid c$
4. $\forall c \neq 0$, $a \mid b$ *iff* $ac \mid bc$
5. If $a \mid b$ and $a \mid c$ then $a \mid sb + tc$ $\forall$ integers s and t

Properties

The following properties are straightforward by applying directly the definitions:

1. If $a \mid b$ then $a \mid bc$ $\forall$ integers c
2. If $a \mid b$ and $b \mid c$ then $a \mid c$
3. If $a \mid b$ and $a \mid b + c$ then $a \mid c$
4. $\forall c \neq 0$, $a \mid b$ *iff* $ac \mid bc$
5. If $a \mid b$ and $a \mid c$ then $a \mid sb + tc$ $\forall$ integers s and t

Proving the last one:

there exist k_1 and k_2 such that $a.k_1 = b$ and $a.k_2 = c$, which implies $a(k_1.s + k_2.t) = sb + tc$ for any s and t.

Greatest Common Divisor

Definition.
$GCD(a, b)$ is the largest number that is a divisor of both a and b.

Proof

Proposition:

$GCD(a, b)$ is equal to the smallest positive linear combination of a and b.[2]

[2] This result is also known as Bezout identity.

Proof

Proposition:

$GCD(a, b)$ is equal to the smallest positive linear combination of a and b.[2]

The proof considers m as the smallest positive linear combination of a and b.

We prove respectively that $m \geq GCD(a, b)$ and $m \leq GCD(a, b)$ by using the general previous properties.

[2] This result is also known as Bezout identity.

$m \geq GCD(a, b)$

By definition, $GCD(a, b) \mid a$ and $GCD(a, b) \mid b$,
then, $GCD(a, b) \mid sa + tb$ for any s and t (and thus, in particular for the smallest combination).
Then, $GCD(a, b)$ divides m and $m \geq GCD(a, b)$.

$m \leq GCD(a, b)$

First, remark that $m \leq a$ because $a = 1.a + 0.b$ is a particular linear combination.
We show that $m \mid a$.

By the division theorem[3], there exists a decomposition $a = q.m + r$ (where $0 \leq r < m$).

[3] whose proof will be detailed later

$m \leq GCD(a, b)$

First, remark that $m \leq a$ because $a = 1.a + 0.b$ is a particular linear combination.
We show that $m \mid a$.

By the division theorem[3], there exists a decomposition $a = q.m + r$ (where $0 \leq r < m$).
Recall also that $m = sa + tb$ for some s and t.
Thus, r can be written as $a - q.m = (1 - qs)a + (-qt)b$ which is a linear combination of a and b.

[3] whose proof will be detailed later

$m \leq GCD(a, b)$

First, remark that $m \leq a$ because $a = 1.a + 0.b$ is a particular linear combination.
We show that $m \mid a$.

By the division theorem[3], there exists a decomposition $a = q.m + r$ (where $0 \leq r < m$).
Recall also that $m = sa + tb$ for some s and t.
Thus, r can be written as $a - q.m = (1 - qs)a + (-qt)b$ which is a linear combination of a and b.
However, as m is the smallest one and $r < m$, we get $r = 0$.

[3] whose proof will be detailed later

$m \leq GCD(a, b)$

First, remark that $m \leq a$ because $a = 1.a + 0.b$ is a particular linear combination.
We show that $m \mid a$.

By the division theorem[3], there exists a decomposition $a = q.m + r$ (where $0 \leq r < m$).
Recall also that $m = sa + tb$ for some s and t.
Thus, r can be written as $a - q.m = (1 - qs)a + (-qt)b$ which is a linear combination of a and b.
However, as m is the smallest one and $r < m$, we get $r = 0$.

Symmetrically m divides also b.
Then, $m \leq GCD(a, b)$.

[3] whose proof will be detailed later

An important result

Corollary.

Every linear combination of a and b is a multiple of $GCD(a, b)$ and vice-versa.

An important result

Corollary.

Every linear combination of a and b is a multiple of $GCD(a, b)$ and vice-versa.

Properties of the GCD

- Every common divisor of a and b divides GCD(a,b)
- GCD(ak,bk)=k.GCD(a,b) for all $k > 0$
- if GCD(a,b)=1 and GCD(a,c)=1 then GCD(a,bc)=1
- if $a \mid bc$ and GCD(a,b)=1 then $a \mid c$
- GCD(a,b) = GCD(b,rem(a,b))

Euclid's Algorithm

Proposition.

GCD(a,b) = GCD(b,rem(a,b))

rem denotes the reminder of the euclidian division of a by b.

The property is useful for quickly – iteratively – compute the *GCD* of two numbers.

Geometric interpretation

- Could you provide the proof?

Geometric interpretation

- Could you provide the proof?

Attention!
A picture is an insight,
this is NOT a proof.

Proof

The idea is to show that the set of common divisors of a and b (called D) is equal to the set of the common divisors of b and $rem(a, b)$ (called D').

Proof

The idea is to show that the set of common divisors of a and b (called D) is equal to the set of the common divisors of b and $rem(a, b)$ (called D').

- If $d \in D$, $d \mid a$ and $d \mid b$.
  As $a = q.b + rem(a, b)$, we have $d \mid rem(a, b)$.
  Then, $d \in D'$.
- If $d' \in D'$, $d' \mid b$ and $d' \mid rem(a, b)$.
  d' divides any linear combination of them, in particular
  $q.b + 1.rem(a, b)$
  thus, $d' \mid a$ which proves that $d' \in D$.

The division theorem

Divisibility is not always perfect.

- If one number does not evenly divide another, there is a remainder left.

Division theorem.

Let a and b be two integers such that $b > 0$, then there exists a unique pair of integers q and r such that $a = qb + r$ and $0 \leq r < b$.

Proving this theorem is two-fold: first the existence, and then the uniqueness.

Existence

Let E be the set of all positive integers in the form $n = a - bz$.
E is not empty (for instance, it contains a) and $E \subset N$, thus, it has a smallest element, say r.
Proving $r < b$ is easy by remarking that $r = a - bz$ for some z and $r - b$ does not belong to E because r is the smallest one.
Thus, $r - b < 0$.

Uniqueness

Let us prove this part by contradiction[4].

Suppose there exist two such pairs of integers:
$a = q_i.b + r_i$ for $i = 1, 2$.
Then, $(q_1 - q_2).b + r_1 - r_2 = 0$.
Thus, b divides $r_1 - r_2$ and $0 \leq r_1 < b$ and $0 \leq r_2 < b$
$r_1 - r_2 = 0$ and thus, $q_1 = q_2$.

[4] that is common for this kind of proof

Primes

Definition.
A *prime* is an integer with no positive divisor other than 1 and itself (otherwise, it is said a *composite*).
1 is neither a prime nor a composite.

Fundamental theorem of Arithmetic.
Every positive integer n can be written in an unique way as a product of primes: $n = p_1 p_2 ... p_j$ $(p_1 \leq p_2 \leq ... \leq p_j)$.

We have again two results to prove: first that every integer can be written as the product of primes, and second that this factorization is unique.

Proof (existence)

The first part is proved easily by a strong induction:
Let assume that all numbers can be decomposed accordingly up to n and let consider $n + 1$.

- If it is prime the decomposition exists (it is it-self)
- if it is a composite, each factor can be expressed as a product of primes by the induction hypothesis.

Proof (uniqueness)

The uniqueness is obtained by contradiction:
Let us first order the primes of the decomposition by increasing values.

$$P_1 < P_2 < \cdots < P_{r-1} < P_r$$

where $P_i \leq n$.
Assume n has two distinct canonical prime factorizations.

$$\langle a_1, a_2, \ldots, a_r \rangle \quad \text{and} \quad \langle b_1, b_2, \ldots, b_r \rangle$$

such that n is expressible by – i.e., is equal to – both of the following products of the primes P_1, P_2, ..., P_{r-1}, P_r.

$$P_1^{a_1} \cdot P_2^{a_2} \cdot \ \ldots \ \cdot P_{r-1}^{a_{r-1}} \cdot P_r^{a_r} \tag{1}$$

$$P_1^{b_1} \cdot P_2^{b_2} \cdot \ \ldots \ \cdot P_{r-1}^{b_{r-1}} \cdot P_r^{b_r} \tag{2}$$

Let us now cancel the longest common prefix.

Because the two products are, by hypothesis, distinct, at least one of them will not be reduced to 1 by this cancellation. We are, therefore, left with residual products of the forms

$$P_i^{a_i} \cdot X \tag{3}$$

$$P_i^{b_i} \cdot Y \tag{4}$$

- Precisely one of a_i and b_i equals 0. Say, $b_i = 0$ while $a_i \neq 0$.
- Products X and Y are composed only of primes that are strictly bigger than P_i.

We have reached the **point of contradiction**:

On the one hand, P_i *must* divide the product Y, because it divides the product $P_i^{a_i} \cdot X$ which equals Y.

On the other hand, P_i *cannot* divide the product Y, because every prime factor of Y is bigger than P_i (and a prime cannot divide a bigger prime).

3 examples

- Perfect numbers
- Little Fermat theorem
- When Fibonacci meets GCD

Perfect Numbers

Theorem

For every Mersenne-prime $2^p - 1$, the number

$$2^{p-1} \cdot (2^p - 1) = \binom{2^p}{2} \tag{5}$$

is perfect.

Perfect Numbers

Theorem

For every Mersenne-prime $2^p - 1$, the number

$$2^{p-1} \cdot (2^p - 1) = \binom{2^p}{2} \tag{5}$$

is perfect.

With the aid of the Fundamental Theorem of Arithmetic, let us enumerate the factors of $2^{p-1} \cdot (2^p - 1)$

The list consists of two groups:

1. all powers of 2, from $2^0 = 1, \ldots, 2^{p-1}$;
2. all products: $(2^p - 1) \times$(a power of 2 from $2^0 = 1, \ldots, 2^{p-2}$).

Fermat's Little Theorem

Aside from its exposing an important and basic property of prime numbers, the theorem provides the basis for a valuable algorithm for testing the primality of integers.

Theorem

Let a be any integer, and let p be any prime.

(1): The number $a^p - a$ is divisible by p.

(2): $a^p \equiv a \bmod p$.

Proof (sketches)

We provide two proofs for this fundamental result, each providing rather different insights on the result.

We focus on a fixed prime p and argue by induction on the alphabet size a, that $a^p \equiv a \bmod p$.
We assume for **induction** that $a^p \equiv a \bmod p$ for all alphabet sizes not exceeding the integer b.

Invoking the restricted form of the Binomial Theorem, we know that

$$(b+1)^p \;=\; (b^p+1) \;+\; \sum_{i=1}^{p-1} \binom{p}{i} b^{p-i} \tag{6}$$

A pictorial argument...

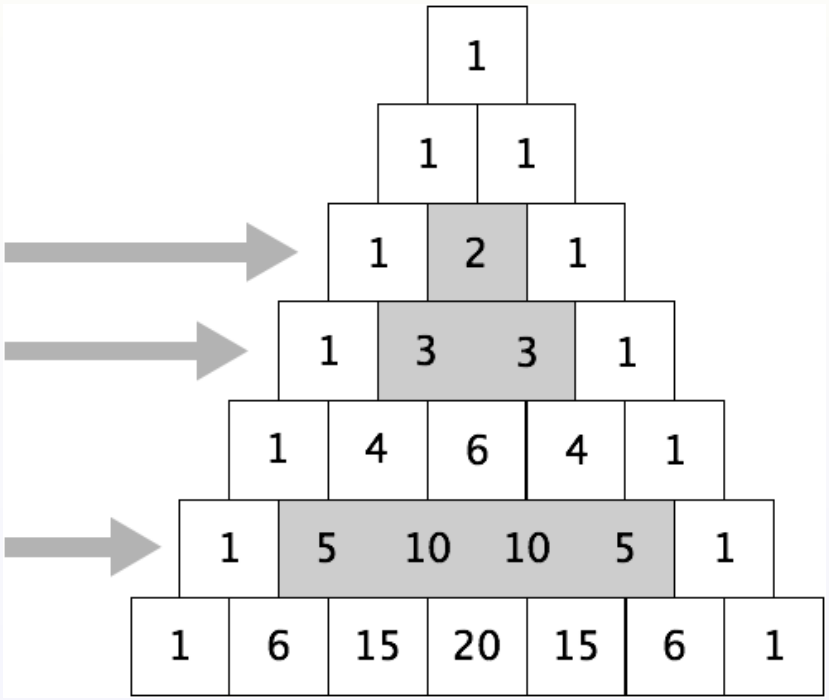


Figure: The "internal" entries of the rows that correspond to prime numbers (in this case, $n = 2$, $n = 3$, and $n = 5$) are divisible by that number.

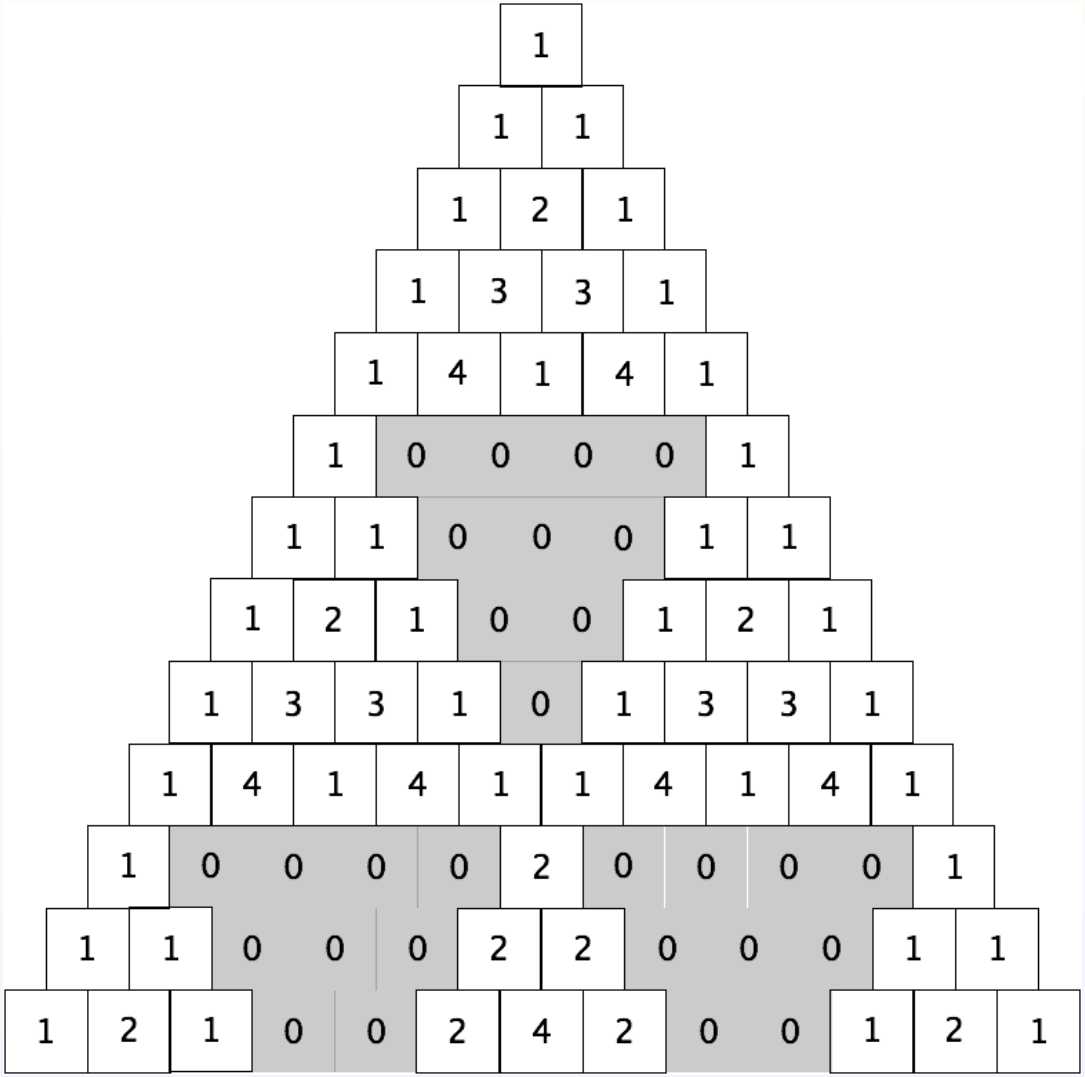


Figure: Pascal's triangle module a prime (5).

A fractal structure

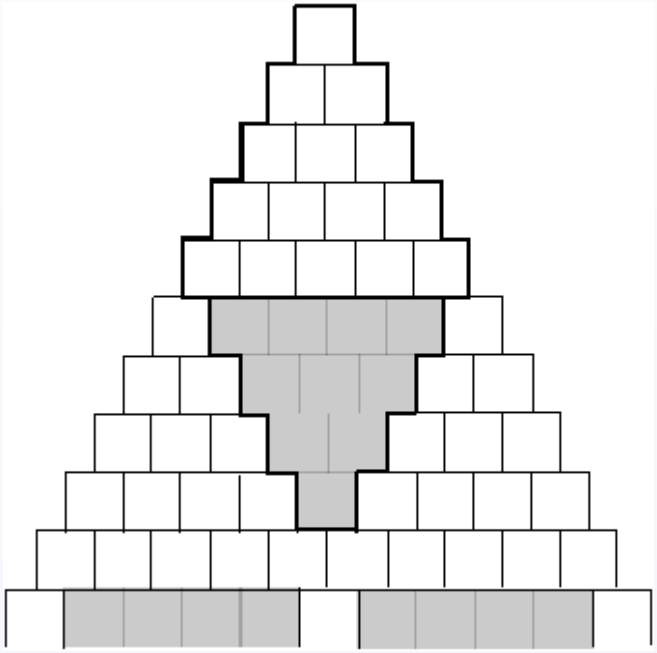
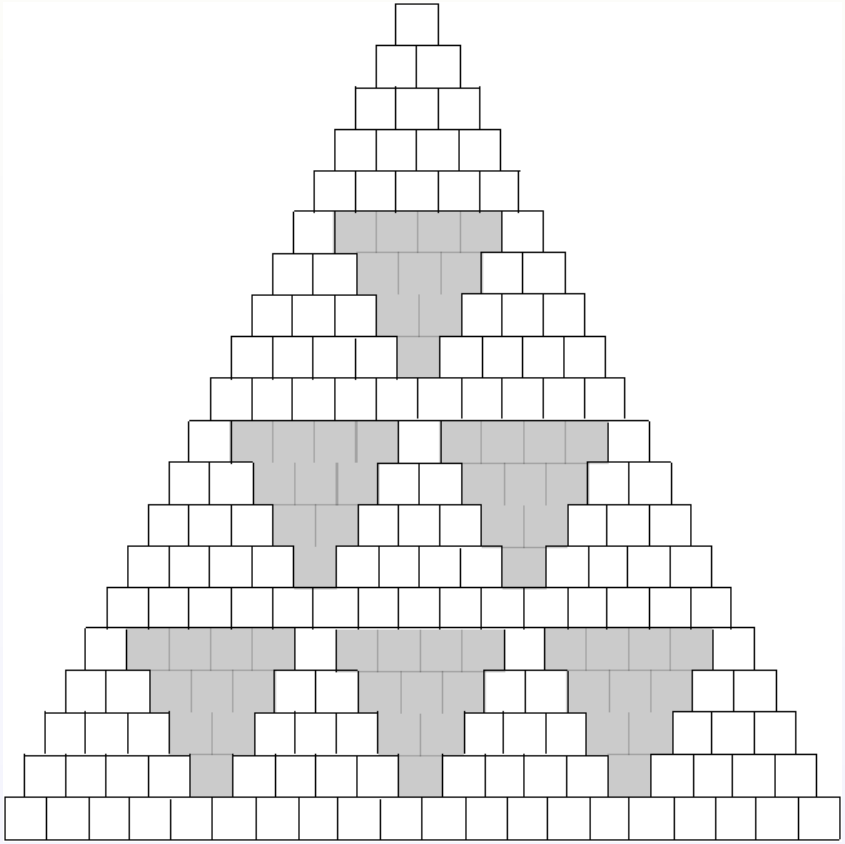


Figure: The shaded area corresponds to 0.



Final touch

Completing the proof is not difficult.

It is let to the reader as a training exercise.

An alternative (combinatorial) proof

a and p be as in the theorem, consider the set of all words/strings of length p over an alphabet/set $\{\alpha_1, \alpha_2, \ldots, \alpha_a\}$ of a symbols. For instance, when on the binary alphabet $\{0, 1\}$ (so that $a = 2$) and $p = 3$, the set consists of the words:

$$000,\ 001,\ 010,\ 011,\ 100,\ 101,\ 110,\ 111$$

Except the two groups with the same symbols (000 and 111), there are two groups of size $p = 3$ (namely, the group with one 1 and the group with two 1s).

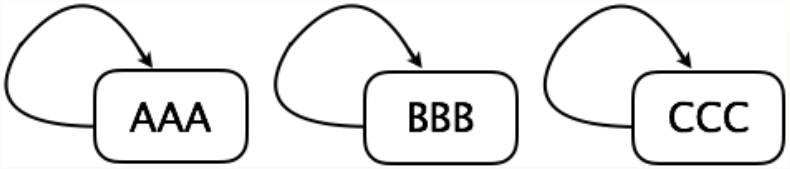


Figure: The 3 necklaces composed of the same symbol ($a = 3$)

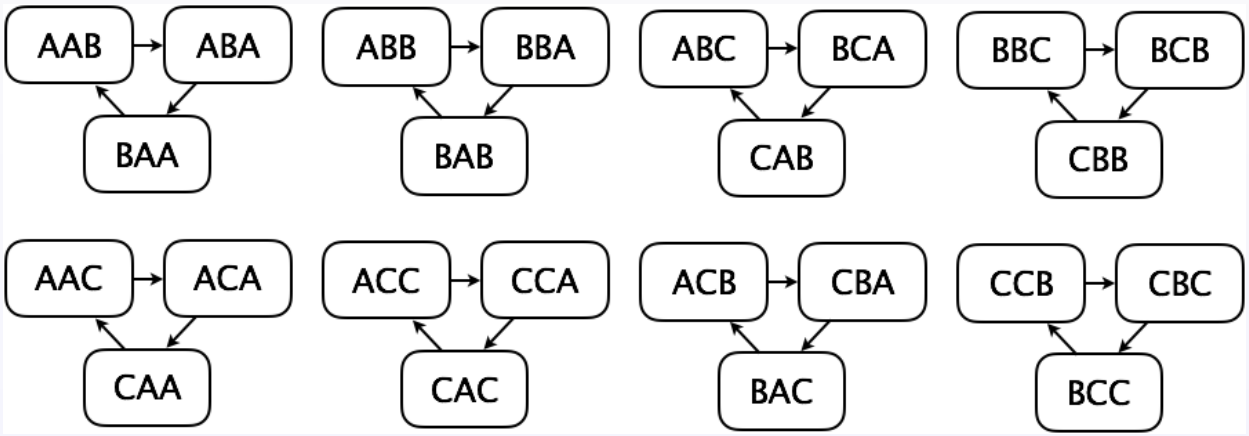


Figure: 2^3 groups of necklaces of size $p = 3$ (for $a = 3$).

When divisibility meets Fibonacci numbers...

Let $F(1) = F(2) = 1$ and $F(n+1) = F(n) + F(n-1)$.

Theorem
$GCD(F(n), F(m)) = F(GCD(n, m))$.

Without loss of generality, consider that $n \geq m$.

Gaining intuition

Recall the Fibonacci progression:
$F(1) = F(2) = 1, F(3) = 2, F(4) = 3, F(5) = 5, F(6) = 8, F(7) = 13, F(8) = 21, F(9) = 34, F(10) = 55, \cdots$

Examples:

$GCD(F(6), F(8)) = GCD(8, 21) = 1$
$F(GCD(6, 8)) = F(2) = 1$

$GCD(F(5), F(10)) = GCD(5, 55) = 5$
$F(GCD(5, 10)) = F(5) = 5$

$GCD(F(12), F(18)) = GCD(144, 2584) = 8$
$F(GCD(12, 18)) = F_6 = 8.$

Proof

Say, with no loss of generality, that $n \geq m$.
Our proof builds on the development of GCD:

$$\mathrm{GCD}(F(n), F(m)) \;=\; \mathrm{GCD}(F(m), F(\mathrm{REM}(n, m)))$$

Three technical Lemma

- The following relation holds for any integers n and $k \geq 1$

$$F(n+k) \;=\; F(k) \cdot F(n+1) \;+\; F(k-1) \cdot F(n)$$

  Hint: The proof is a straightforward induction on k for fixed n.

- For any integer $k \geq 1$, $F(n)$ divides $F(k \cdot n)$
  Hint: The proof is obtained by induction on k by writing
  $F((k+1) \cdot n) = F(n + k \cdot n) =$
  $F(k \cdot n) \cdot F(n+1) \;+\; F(k \cdot n - 1) \cdot F(n)$

- For any integer $n \geq 1$, $F(n)$ and $F(n-1)$ are relatively prime:

$$\mathrm{GCD}(F(n-1), F(n)) \;=\; 1$$

  Hint: The proof is a straightforward induction.

We are now able to verify identity via the following assertions, where $r = \text{REM}(m, n)$.

$\text{GCD}(F(n), F(m))$

$$\begin{aligned}
&= \text{GCD}(F(q \cdot m + r), F(m)) \\
&= \text{GCD}(F(m),\ F(m \cdot q + 1) \cdot F(r)\ +\ F(m \cdot q) \cdot F(r - 1)) \\
&= \text{GCD}(F(m),\ F(m \cdot q + 1) \cdot F(r)) \\
&= \text{GCD}(F(m),\ F(r))
\end{aligned}$$

The final touch

Applying this process until $r = 0$ completes the proof.
The last Fibonacci number we have obtained is
$F\left(\mathrm{GCD}(m, n)\right)$.