

# The Fibonacci Sequence

Thomas Browning

March 2018

## Contents

<b>1</b>	<b>The Fibonacci Sequence</b>	<b>2</b>
1.1	Domino Tilings . . . . .	2
1.2	Divisibility of Fibonacci Numbers . . . . .	2
1.3	The Greatest Common Divisor . . . . .	4
1.4	Fibonacci Entry Points . . . . .	4
1.5	A Formula . . . . .	5
1.6	Finite fields . . . . .	6
1.7	Field Extensions . . . . .	7
1.8	Quadratic Reciprocity . . . . .	9
1.9	An Example . . . . .	11

# 1 The Fibonacci Sequence

## 1.1 Domino Tilings

Let  $T_n$  count the number of ways to tile a  $2 \times n$  board with dominos. We will set  $T_{-1} = 0$  and  $T_0 = 1$ . The first few values of  $T_n$  are given in Figure 1 below.

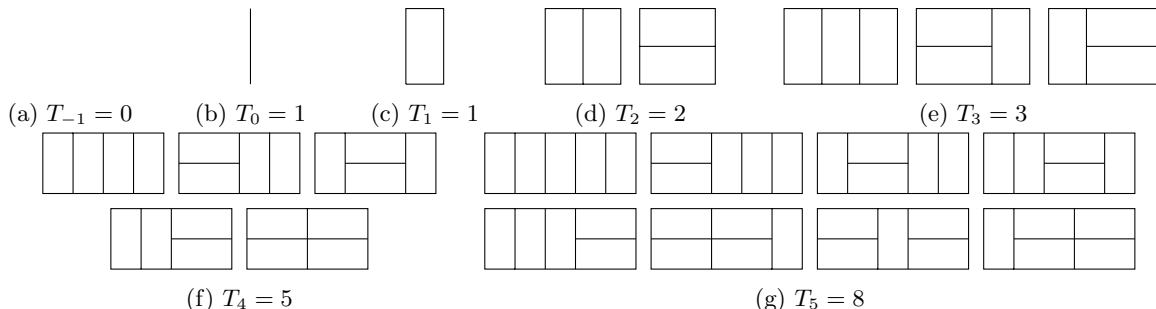


Figure 1: Values of  $T_n$  for small  $n$

Let  $m$  and  $n$  be nonnegative integers. Every tiling of a  $2 \times (m + n)$  board with dominos will either have a break between the first  $m$  columns and the last  $n$  columns or will have two horizontal dominos lying over the line between the first  $m$  columns and the last  $n$  columns. In the first case there are  $T_m$  ways to tile the left side of the board and there are  $T_n$  ways to tile the right side of the board. In the second case there are  $T_{m-1}$  ways to tile the left side of the board and there are  $T_{n-1}$  ways to tile the right side of the board. This is shown pictorially in Figure 2 below.

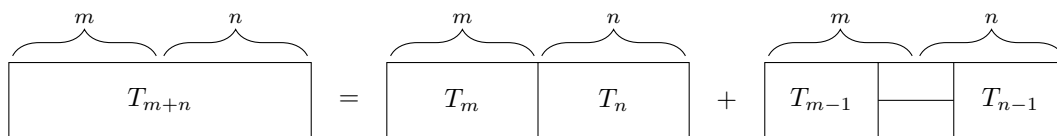


Figure 2: Cutting the board

Adding up the number of tilings from each of the two cases gives the recursive formula

$$T_{m+n} = T_m T_n + T_{m-1} T_{n-1} \text{ for } m, n \geq 0. \quad (1.1)$$

In the special case where  $m = 1$ , Equation 1.1 reduces to the recursive formula

$$T_{n+1} = T_n + T_{n-1} \text{ for } n \geq 0. \quad (1.2)$$

You might be worried about Equation 1.1 when  $m = 0$  or  $n = 0$ . Don't worry: if  $m = 0$  then Equation 1.1 reduces to the tautology  $T_n = T_n$ . Similarly, if  $n = 0$  then Equation 1.1 reduces to the tautology  $T_m = T_m$ .

## 1.2 Divisibility of Fibonacci Numbers

We define the shifted sequence  $F_n = T_{n-1}$  which will be easier to work with in the long run. The number  $F_n$  is called the  $n$ th Fibonacci number. The motivating goal of this first chapter is the understand the prime factorization of Fibonacci numbers. The first 150 Fibonacci numbers are given in Table 1 and factorizations

of the first 100 Fibonacci numbers are given in Table 2. Careful examination of Table 2 suggests the patterns

- Every 3rd Fibonacci number is divisible by 2
- Every 4th Fibonacci number is divisible by 3
- Every 6th Fibonacci number is divisible by 4
- Every 5th Fibonacci number is divisible by 5
- Every 12th Fibonacci number is divisible by 6
- Every 8th Fibonacci number is divisible by 7
- Every 6th Fibonacci number is divisible by 8
- Every 12th Fibonacci number is divisible by 9
- Every 15th Fibonacci number is divisible by 10

This naturally leads to the following conjecture:

**Conjecture 1.** *For every positive integer  $d$ , there is a positive integer  $a_d$  such that  $F_n$  is divisible by  $d$  if and only if  $n$  is divisible by  $a_d$ . Equivalently, the values of  $n$  such that  $F_n$  is divisible by  $d$  are precisely the nonnegative integer multiples of  $a_d$ .*

The number  $a_d$  in Conjecture 1 is called the  $d$ th Fibonacci entry point. Suppose for a moment that Conjecture 1 is true and let  $c$  and  $d$  have no common divisors other than 1. Then we have the chain of biconditionals

$$\begin{aligned}
 n \text{ is divisible by } a_{cd} &\iff F_n \text{ is divisible by } cd \\
 &\iff F_n \text{ is divisible by both } c \text{ and } d \\
 &\iff n \text{ is divisible by both } a_c \text{ and } a_d \\
 &\iff n \text{ is divisible by } \text{lcm}(a_c, a_d), \text{ the least common multiple of } a_c \text{ and } a_d.
 \end{aligned}$$

Thus,  $a_{cd} = \text{lcm}(a_c, a_d)$ . Repeated application of this result shows that if  $d = p_1^{b_1} \dots p_k^{b_k}$  is the prime factorization of a positive integer  $d$  then we have the identity

$$a_d = \text{lcm}(a_{p_1^{b_1}}, \dots, a_{p_k^{b_k}}).$$

In particular, the values of  $a_d$  for all positive integers  $d$  are determined by the values of  $a_{p^b}$  for all prime powers  $p^b$ . The values of  $a_{p^b}$  for primes  $p \leq 230$  and all  $1 \leq b \leq 5$  are given in Table 3. Careful examination of Table 3 suggests the following conjecture:

**Conjecture 2.** *For all primes  $p$  and all positive integers  $b$ ,*

$$a_{p^b} = \begin{cases} 3 \cdot 2^{b-1} & p = 2, b \leq 2 \\ 3 \cdot 2^{b-2} & p = 2, b \geq 3 \\ p^{b-1} a_p & p \geq 3 \end{cases}$$

If both conjectures are true then the values of  $a_d$  for all positive integers  $d$  are determined by the values of  $a_p$  for all primes  $p$ . Ideally, we would prove Conjectures 1 and 2 and then determine the values of  $a_p$  for all primes  $p$ . Doing so would solve the problem of understanding the prime factorizations of Fibonacci numbers. This plan is far too ambitious. In fact, Conjecture 2 is currently an open problem in mathematics and the values of  $a_p$  for primes  $p$  are not well-understood. Here is what we will do:

- We will prove Conjecture 1 by analyzing the greatest common divisor of Fibonacci numbers.
- We will prove a partial result regarding the values of  $a_p$  for all primes  $p$  (see Corollary 4).

### 1.3 The Greatest Common Divisor

For integers  $m$  and  $n$ , we say that  $m$  divides  $n$  when  $n = km$  for some integer  $k$ . For example 4 divides 20 with  $k = 5$ , 8 divides 8 with  $k = 1$ , and 6 divides 0 with  $k = 0$ . For integers  $m$  and  $n$ , a common divisor of  $m$  and  $n$  is an integer  $d$  such that  $d$  divides  $m$  and  $d$  divides  $n$ . For example, 5 is a common divisor of 20 and 25, 4 is a common divisor of 12 and 24, and 10 is a common divisor of 0 and 20. If  $m$  and  $n$  are not both equal to 0 then  $m$  and  $n$  have only finitely many common divisors. In particular,  $m$  and  $n$  have a greatest common divisor which we denote by  $\gcd(m, n)$ . For example,  $\gcd(20, 25) = 5$ ,  $\gcd(12, 24) = 12$ ,  $\gcd(0, 20) = 20$ .

If  $d$  is a common divisor of both  $m$  and  $km + n$  then  $d$  is a divisor of  $n = (km + n) - km$ . Conversely, if  $d$  is a common divisor of both  $m$  and  $n$  then  $d$  is a divisor of  $km + n$ . This shows that the common divisors of  $m$  and  $km + n$  coincide with the common divisors of  $m$  and  $n$ . In particular, the greatest common divisor of  $m$  and  $km + n$  must equal the greatest common divisor of  $m$  and  $n$ . This shows that

$$\gcd(m, km + n) = \gcd(m, n). \quad (1.3)$$

In the case that  $k = 1$ , Equation 1.3 becomes

$$\gcd(m, n) = \gcd(m - n, n). \quad (1.4)$$

In particular, the greatest common divisor of two positive integers can be computed by repeatedly subtracting the smaller integer from the larger integer until the two integers are equal. This is called the Euclidean algorithm for computing the greatest common divisor.

We now analyze the greatest common divisor of Fibonacci numbers. By Equations 1.2 and 1.3,

$$\gcd(F_{n+1}, F_n) = \gcd(F_n + F_{n-1}, F_n) = \gcd(F_{n-1}, F_n) = \gcd(F_n, F_{n-1})$$

for all  $n \geq 1$ . Since  $\gcd(F_1, F_0) = \gcd(1, 0) = 1$ , this shows that  $\gcd(F_{n+1}, F_n) = 1$  for all  $n \geq 0$ . By Equations 1.1 and 1.3,

$$\gcd(F_m, F_n) = \gcd(F_{m-n-1}F_n + F_{m-n}F_{n+1}, F_n) = \gcd(F_n, F_{m-n-1}F_n + F_{m-n}F_{n+1}) = \gcd(F_n, F_{m-n}F_{n+1})$$

for all  $m > n \geq 0$ . However,  $\gcd(F_{n+1}, F_n) = 1$  so  $F_n$  and  $F_{n+1}$  have no common factors other than 1. As a consequence,

$$\gcd(F_m, F_n) = \gcd(F_n, F_{m-n}F_{n+1}) = \gcd(F_n, F_{m-n}) = \gcd(F_{m-n}, F_n).$$

This is precisely the result of applying one step of the Euclidean algorithm to the indices  $m$  and  $n$ . Repeating this process until the Euclidean algorithm terminates shows that

$$\gcd(F_m, F_n) = F_{\gcd(m, n)} \text{ for all } m, n \geq 0. \quad (1.5)$$

Note that Equation 1.5 is much cleaner in terms of  $F_n$  than in terms of  $T_n$ . This justifies our decision to work with the shifted sequence  $F_n = T_{n-1}$ .

### 1.4 Fibonacci Entry Points

We can now prove Conjecture 1. Fix a positive integer  $d$ . Consider the sequence of the pairs of remainders when dividing  $F_n$  and  $F_{n+1}$  by  $d$ . There are only  $d^2$  possible pairs of remainders so this sequence must eventually repeat. However, Equation 1.2 shows that any term of the sequence determines both the previous term of the sequence and the next term of the sequence. Since the sequence starts at the pair  $(0, 1)$ , the sequence must eventually cycle back to  $(0, 1)$ . This shows that  $F_n$  will be divisible by  $d$  for some positive integer  $n$ . Now consider the collection  $S_d$  of the values of  $n$  such that  $F_n$  is divisible by  $d$ . We have shown that  $S_d$  contains a positive integer. Let  $a_d$  be the smallest positive integer contained in  $S_d$ . For any nonnegative integer multiple  $ka_d$  of  $a_d$ , Equation 1.5 states that

$$\gcd(F_{a_d}, F_{ka_d}) = F_{\gcd(a_d, ka_d)} = F_{a_d}$$

which is divisible by  $d$ . Then  $F_{ka_d}$  is divisible by  $d$  so  $S_d$  contains  $ka_d$ . This shows that that  $S_d$  contains the nonnegative integer multiples of  $a_d$ . For the converse, let  $n$  be an positive integer contained in  $S_d$ . Then  $F_n$  is divisible by  $d$  so  $d$  is a common divisor of  $F_n$  and  $F_{a_d}$ . Equation 1.5 gives that

$$F_{\gcd(a_d, n)} = \gcd(F_{a_d}, F_n)$$

which is divisible by  $d$ . Then  $\gcd(a_d, n) \geq a_d$  by the minimality of  $a_d$ . However,  $\gcd(a_d, n) \leq a_d$  by properties of the greatest common divisor. Thus,  $\gcd(a_d, n) = a_d$  so  $n$  is a nonnegative integer multiple of  $a_d$ . This shows that  $S_d$  is the collection of nonnegative integer multiples of  $a_d$  which proves Conjecture 1.

## 1.5 A Formula

Examining the number of digits of the first 150 Fibonacci numbers suggests that the Fibonacci numbers grow exponentially. Suppose that the sequence  $a_n = x^n$  satisfied the Fibonacci recurrence  $a_{n+2} = a_{n+1} + a_n$  for some fixed real number  $x$ . Setting  $n = 0$  shows that  $x$  is a root of the quadratic polynomial  $x^2 - x - 1$ . Conversely, if  $x$  is a root of the quadratic polynomial  $x^2 - x - 1$  then  $x^{n+2} = x^n(x^2) = x^n(x+1) = x^{n+1} + x^n$  so the exponential sequence  $a_n = x^n$  will satisfy the Fibonacci recurrence  $a_{n+2} = a_{n+1} + a_n$ .

If  $\varphi$  and  $\psi$  are distinct roots of the quadratic polynomial  $x^2 - x - 1$  and if  $c$  and  $d$  are real numbers, then the linear combination sequence  $a_n = c\varphi^n + d\psi^n$  will also satisfy the Fibonacci recurrence  $a_{n+2} = a_{n+1} + a_n$ . If we can choose  $c$  and  $d$  such that  $a_0 = 0$  and  $a_1 = 1$  then it must be the case that  $a_n = F_n$  for all  $n \geq 0$  and we will obtain a formula for the Fibonacci sequence. We would like to choose  $c$  and  $d$  such that  $0 = a_0 = c\varphi^0 + d\psi^0 = c + d$  and such that  $1 = a_1 = c\varphi^1 + d\psi^1 = c\varphi + d\psi$ . The first equation shows that  $d = -c$ . Then the second equation becomes  $1 = c\varphi - c\psi = c(\varphi - \psi)$  which shows that  $c = 1/(\varphi - \psi)$ . Thus, if  $c = 1/(\varphi - \psi)$  and if  $d = -1/(\varphi - \psi)$  then the Fibonacci numbers are given by the formula  $F_n = c\varphi^n + d\psi^n$ . We may also write this formula as

$$F_n = \frac{\varphi^n - \psi^n}{\varphi - \psi}. \quad (1.6)$$

This formula for the Fibonacci numbers works in other number systems. A field to be a set with a 0-element, a 1-element, addition, subtraction, multiplication, and division by nonzero elements. For example, the real numbers are a field and the rational numbers are a field but the integers are not a field. If  $K$  is a field then we can define the Fibonacci numbers in  $K$  by  $F_0 = 0$ ,  $F_1 = 1$ , and  $F_{n+2} = F_{n+1} + F_n$ . Furthermore, suppose that  $\varphi$  and  $\psi$  are distinct roots of the polynomial  $x^2 - x - 1$  in  $K$ . Then Equation 1.6 gives a formula for the Fibonacci numbers in  $K$ . To prove this, note that

$$\frac{\varphi^0 - \psi^0}{\varphi - \psi} = \frac{1 - 1}{\varphi - \psi} = 0, \quad \frac{\varphi^1 - \psi^1}{\varphi - \psi} = \frac{\varphi - \psi}{\varphi - \psi} = 1, \quad \frac{\varphi^{n+2} - \psi^{n+2}}{\varphi - \psi} = \frac{\varphi^{n+1} - \psi^{n+1}}{\varphi - \psi} + \frac{\varphi^n - \psi^n}{\varphi - \psi}$$

where the last equality holds since  $\varphi^{n+2} = \varphi^n(\varphi^2) = \varphi^n(\varphi + 1) = \varphi^{n+1} + \varphi^n$  and similarly for  $\psi$ .

We have shown that if the polynomial  $x^2 - x - 1$  has two distinct roots in the field  $K$  then Equation 1.6 gives a formula for the Fibonacci numbers in  $K$ . It is natural to ask when this hypothesis holds. We will suppose for now that  $2 \neq 0$  in  $K$  (meaning that  $1 + 1 \neq 0$  in  $K$ ) and that  $5 \neq 0$  in  $K$  (meaning that  $1 + 1 + 1 + 1 + 1 \neq 0$  in  $K$ ). If  $K$  contains a square root of 5 then we have that

$$\left(\frac{1 \pm \sqrt{5}}{2}\right)^2 = \frac{(1 \pm \sqrt{5})^2}{4} = \frac{1 \pm 2\sqrt{5} + 5}{4} = \frac{3 \pm \sqrt{5}}{2} = \frac{1 \pm \sqrt{5}}{2} + 1.$$

This shows that the two values  $(1 \pm \sqrt{5})/2$  are roots of  $x^2 - x - 1$  in  $K$ . In fact, these two values are distinct since their difference is  $\sqrt{5}$  which is nonzero since  $5 \neq 0$  by assumption. Conversely, suppose that there exist distinct roots  $\varphi$  and  $\psi$  of  $x^2 - x - 1$  in  $K$ . I claim that this gives a factorization  $x^2 - x - 1 = (x - \varphi)(x - \psi)$ .

*Proof using polynomial division:* We may apply the polynomial division algorithm to write

$$x^2 - x - 1 = q(x)(x - \psi) + r(x)$$

where  $q(x)$  is a polynomial of degree 1 (a linear polynomial) and where  $r(x)$  is a polynomial of degree 0 (a constant polynomial). Substituting  $x = \psi$  gives that

$$0 = \psi^2 - \psi - 1 = q(\psi)(\psi - \psi) + r(\psi) = r(\psi).$$

However,  $r(x)$  is a constant polynomial so  $r(x) = 0$  and we have that  $x^2 - x - 1 = q(x)(x - \psi)$ . Substituting  $x = \varphi$  gives that

$$0 = \varphi^2 - \varphi - 1 = q(\varphi)(\varphi - \psi)$$

where  $\varphi - \psi \neq 0$  since  $\varphi \neq \psi$  by assumption. Then  $q(\varphi) = 0$ . However,  $q(x)$  is a linear polynomial so  $q(x) = c(x - \varphi)$  for some constant  $c$ . Comparing leading coefficients of the equality  $x^2 - x - 1 = c(x - \varphi)(x - \psi)$  shows that  $c = 1$  as claimed.  $\square$

We now have the factorization  $x^2 - x - 1 = (x - \varphi)(x - \psi)$ . Comparing coefficients gives that  $\varphi + \psi = 1$  and that  $\varphi\psi = -1$ . Then

$$(\varphi - \psi)^2 = \varphi^2 + \psi^2 - 2\varphi\psi = (\varphi + 1) + (\psi + 1) + 2 = (\varphi + \psi) + 4 = 5$$

so  $K$  contains a square root of 5. We summarize these results in the following proposition:

**Proposition 1.** *Let  $K$  be a field. If  $\varphi$  and  $\psi$  are distinct roots of the polynomial  $x^2 - x - 1$  in  $K$  then Equation 1.6 gives a formula for the Fibonacci numbers in  $K$ . If  $2 \neq 0$  in  $K$  and if  $5 \neq 0$  in  $K$  then the polynomial  $x^2 - x - 1$  has distinct roots in  $K$  if and only if  $K$  contains a square root of 5.*

If  $K$  is a field and if  $\varphi$  and  $\psi$  are distinct roots of the polynomial  $x^2 - x - 1$  in  $K$  then Equation 1.6 holds. Then  $F_n = 0$  if and only if  $\varphi^n - \psi^n = 0$  if and only if  $\varphi^n = \psi^n$  if and only if  $\varphi^n/\psi^n = 1$  if and only if  $(\varphi/\psi)^n = 1$ . Then Proposition 1 gives the following corollary:

**Corollary 1.** *Let  $K$  be a field. If  $2 \neq 0$  in  $K$  and if  $5 \neq 0$  in  $K$  and if  $K$  contains a square root of 5 then  $F_n = 0$  in  $K$  if and only if  $(\varphi/\psi)^n = 1$  where  $\varphi$  and  $\psi$  are distinct roots of the polynomial  $x^2 - x - 1$  in  $K$ .*

## 1.6 Finite fields

Let  $p$  be a prime. We shall construct a field  $\mathbb{F}_p$  such that  $F_n$  is divisible by  $p$  if and only if  $F_n = 0$  in  $\mathbb{F}_p$ . Let  $\mathbb{F}_p$  consist of the  $p$  distinct remainders when dividing modulo  $p$ . Then 0 is the remainder of numbers that are a multiple of  $p$  and 1 is the remainder of numbers that are 1 more than a multiple of  $p$ . Also, note that addition, subtraction, and multiplication preserve remainders. In the more familiar case where  $p = 10$ , this is just saying that the last digit of a sum, difference, or product is determined by the last digits of the two starting numbers. This shows that we have a well defined addition, subtraction, and multiplication on  $\mathbb{F}_p$ .

To show that we have division by nonzero elements, it suffices to show that nonzero elements have inverses since we can write  $a/b = (a)(b^{-1})$ . Equivalently, it suffices to show that if  $x$  is an integer not divisible by  $p$  (the remainder is nonzero) then there exists an integer  $y$  such that  $xy$  is 1 more than a multiple of  $p$  (the remainder is 1). To see this, consider the  $p - 1$  integers  $x, 2x, \dots, (p - 1)x$ . These  $p - 1$  integers are not divisible by  $p$  so the remainders of these  $p - 1$  integers lie in the  $p - 1$  nonzero remainders modulo  $p$ . If we can show that no two of these  $p - 1$  integers have the same remainder modulo  $p$  then it will follow that each of the  $p - 1$  nonzero remainders modulo  $p$  is the remainder of one of these  $p - 1$  integers. In particular, one of these  $p - 1$  integers will have a remainder of 1 modulo  $p$  which is what we want to show. If  $jx$  and  $kx$  have the same remainder modulo  $p$  for some  $1 \leq j \leq p - 1$  and  $1 \leq k \leq p - 1$  with  $j \neq k$  then  $jx - kx = (j - k)x$  will be divisible by  $p$  where neither  $j - k$  nor  $x$  is divisible by  $p$ . This is a contradiction to prime factorization. We conclude that we have division by nonzero elements.

In summary, we have shown that the collection  $\mathbb{F}_p$  of the  $p$  distinct remainders when dividing modulo  $p$  form a field. Also, the Fibonacci sequence in  $\mathbb{F}_p$  will consist of the remainders of the standard Fibonacci sequence modulo  $p$ . In particular,  $F_n$  is divisible by  $p$  if and only if  $F_n = 0$  in  $\mathbb{F}_p$ . Then Corollary 1 proves the following theorem:

**Theorem 1.** *Let  $p \neq 2, 5$  be a prime and suppose that  $\mathbb{F}_p$  contains a square root of 5. Then  $F_n$  is divisible by  $p$  if and only if  $(\varphi/\psi)^n = 1$  in  $\mathbb{F}_p$  where  $\varphi$  and  $\psi$  are distinct roots of the polynomial  $x^2 - x - 1$  in  $\mathbb{F}_p$ .*

As an example, let  $p = 29$ . Then  $11^2 = 121 = 4 \cdot 29 + 5$  so 11 is a square root of 5 in  $\mathbb{F}_p$ . As shown in the previous section, the two distinct roots of  $x^2 - x - 1$  are given by  $(1 \pm \sqrt{5})/2 = (1 \pm 11)/2$ . These are  $\varphi = (1 - 11)/2 = -10/2 = -5 = 24$  and  $\psi = (1 + 11)/2 = 12/2 = 6$ . The ratio  $\varphi/\psi = 24/6 = 4$  happens to be easy to compute in this case. Thus,  $F_n$  is divisible by 29 if and only if  $4^n$  is one more than a multiple of 29. If we examine the remainders of  $4^n$  modulo 29, we get the sequence

$n$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	...
$4^n$	1	4	16	6	24	9	7	28	25	13	23	5	20	22	1	4	16	...

This sequence is periodic since each entry depends only on the previous entry (multiplication by 4 in  $\mathbb{F}_p$ ). Thus, every 14th Fibonacci number is divisible by 29. Table 3 confirms that  $a_{29} = 14$ .

Let  $a$  be a positive integer. Then  $a^p$  counts the number of ways to color  $p$  spots around a circle with  $a$  colors. We say that a coloring is nonconstant if the coloring uses at least 2 colors. Then  $a^p - a$  counts the number of nonconstant colorings of  $p$  spots around a circle with  $a$  colors. However, given any nonconstant coloring, the  $p$  rotations of this coloring will give  $p$  distinct nonconstant colorings (this is because  $p$  is prime). In particular, we may group the  $a^p - a$  nonconstant colorings into groups of size  $p$  consisting of nonconstant colorings that are the same up to rotation. This shows that  $a^p - a$  is divisible by  $p$ . Taking remainders modulo  $p$  shows that  $a^p - a = 0$  for all elements  $a$  of  $\mathbb{F}_p$ . Equivalently,  $a^p = a$  for all elements  $a$  of  $\mathbb{F}_p$ . If  $a$  is nonzero in  $\mathbb{F}_p$  then dividing by  $a$  shows that  $a^{p-1} = 1$  for all nonzero elements  $a$  of  $\mathbb{F}_p$ . We have shown the following lemma:

**Lemma 1.** *Every element  $a$  of  $\mathbb{F}_p$  satisfies  $a^p = a$ . Every nonzero element  $a$  of  $\mathbb{F}_p$  satisfies  $a^{p-1} = 1$ .*

Combining Theorem 1 with Lemma 1 proves the following corollary:

**Corollary 2.** *Let  $p \neq 2, 5$  be a prime and suppose that  $\mathbb{F}_p$  contains a square root of 5. Then  $F_{p-1}$  is divisible by  $p$ . Equivalently,  $a_p$  divides  $p - 1$ .*

## 1.7 Field Extensions

Let  $p$  be a prime. We now have a good understanding of when  $F_n$  is divisible by  $p$  in the case where  $\mathbb{F}_p$  contains a square root of 5. However, if  $\mathbb{F}_p$  does not contain a square root of 5 then Corollary 1 does not apply to  $\mathbb{F}_p$ . In this case we must consider a field extension. Let  $\mathbb{F}_p(\sqrt{5})$  denote the collection of formal sums  $a + b\sqrt{5}$  for  $a, b \in \mathbb{F}_p$ . To see that this is field, note that we have the 0 element  $0 = 0 + 0\sqrt{5}$ , the 1 element  $1 = 1 + 0\sqrt{5}$ , we have the addition

$$(a + b\sqrt{5}) + (c + d\sqrt{5}) = (a + c) + (b + d)\sqrt{5},$$

we have the subtraction

$$(a + b\sqrt{5}) - (c + d\sqrt{5}) = (a - c) + (b - d)\sqrt{5},$$

we have the multiplication

$$(a + b\sqrt{5})(c + d\sqrt{5}) = ac + ad\sqrt{5} + bc\sqrt{5} + 5bd = (ac + 5bd) + (ad + bc)\sqrt{5},$$

and we have the division

$$\frac{a + b\sqrt{5}}{c + d\sqrt{5}} = \frac{(a + b\sqrt{5})(c - d\sqrt{5})}{(c + d\sqrt{5})(c - d\sqrt{5})} = \frac{(ac - 5bd) + (bc - ad)\sqrt{5}}{c^2 - 5d^2} = \frac{ac - 5bd}{c^2 - 5d^2} + \frac{bc - ad}{c^2 - 5d^2}\sqrt{5}$$

for  $c + d\sqrt{5} \neq 0 + 0\sqrt{5}$ . To see that  $c^2 - 5d^2$  is nonzero, note that if  $d = 0$  then  $c^2 - 5d^2 = c^2$  is nonzero and if  $d \neq 0$  then  $c^2 - 5d^2 = d^2((c/d)^2 - 5)$  is nonzero by our assumption that  $\mathbb{F}_p$  does not contain a square root

of 5. The reader familiar with complex numbers should observe that this same construction can be used to define the complex numbers as  $\mathbb{R}(\sqrt{-1})$  where  $\mathbb{R}$  denotes the real numbers. However, unlike the complex numbers, there still exist polynomials with coefficients in  $\mathbb{F}_p$  that do not factor in  $\mathbb{F}_p(\sqrt{5})$ .

Note that the field  $\mathbb{F}_p(\sqrt{5})$  has a square root of 5 by construction. Then Corollary 1 proves the following theorem:

**Theorem 2.** *Let  $p \neq 2, 5$  be a prime and suppose that  $\mathbb{F}_p$  does not contain a square root of 5. Then  $F_n$  is divisible by  $p$  if and only if  $(\varphi/\psi)^n = 1$  in  $\mathbb{F}_p(\sqrt{5})$  where  $\varphi$  and  $\psi$  are distinct roots of the polynomial  $x^2 - x - 1$  in  $\mathbb{F}_p(\sqrt{5})$ .*

As an example, let  $p = 13$ . Then it can be verified that  $\mathbb{F}_p$  does not have a square root of 5. The two distinct roots of  $x^2 - x - 1$  are given by  $(1 \pm \sqrt{5})/2 = 7 \pm 7\sqrt{5}$ . These are  $\varphi = 7 - 7\sqrt{5} = 7 + 6\sqrt{5}$  and  $\psi = 7 + 7\sqrt{5}$ . We can compute the ratio

$$\frac{\varphi}{\psi} = \frac{7 - 7\sqrt{5}}{7 + 7\sqrt{5}} = \frac{1 - \sqrt{5}}{1 + \sqrt{5}} = \frac{(1 - \sqrt{5})^2}{(1 - \sqrt{5})(1 + \sqrt{5})} = \frac{1 - 2\sqrt{5} + 5}{1 - 5} = \frac{10 + \sqrt{5}}{2} = 5 + 7\sqrt{5}.$$

Thus,  $F_n$  is divisible by 13 if and only if  $(5 + 7\sqrt{5})^n = 1$  in  $\mathbb{F}_p(\sqrt{5})$ . If we examine the remainders of  $(5 + 7\sqrt{5})^n$ , we get the sequence

$n$	0	1	2	3	4	5	6	7	8	...
$(5 + 7\sqrt{5})^n$	1	$5 + 7\sqrt{5}$	$10 + 5\sqrt{5}$	$4 + 4\sqrt{5}$	$4 + 9\sqrt{5}$	$10 + 8\sqrt{5}$	$5 + 6\sqrt{5}$	1	$5 + 7\sqrt{5}$	...

This sequence is periodic since each entry depends only on the previous entry (multiplication by  $5 + 7\sqrt{5}$  in  $\mathbb{F}_p(\sqrt{5})$ ). Thus, every 7th Fibonacci number is divisible by 13. Table 3 confirms that  $a_{13} = 7$ .

A field automorphism of a field  $K$  is a bijection (a permutation or rearrangement)  $f: K \rightarrow K$  that preserves addition and multiplication in the sense that  $f(x + y) = f(x) + f(y)$  and  $f(xy) = f(x)f(y)$  for all elements  $x$  and  $y$  in  $K$ . Furthermore, this definition also implies that

- $f(0) = f(0 + 0) = f(0) + f(0)$  so  $f(0) = 0$ ,
- $f(1) = f(1 \cdot 1) = f(1)f(1)$  so  $f(1) = 1$ ,
- $0 = f(0) = f(x - x) = f(x) + f(-x)$  so  $f(-x) = -f(x)$ ,
- $1 = f(1) = f(xx^{-1}) = f(x)f(x^{-1})$  so  $f(x^{-1}) = f(x)^{-1}$ .

In particular, a field automorphism must preserve all of the structure of the field.

We now exhibit two field automorphisms of  $\mathbb{F}_p(\sqrt{5})$  and show that they are the same. First, consider the conjugation map given by  $\overline{a + b\sqrt{5}} = a - b\sqrt{5}$ . To see that this function is a field automorphism, note that

$$\left(\overline{a + b\sqrt{5}}\right) + \left(\overline{c + d\sqrt{5}}\right) = \left(a - b\sqrt{5}\right) + \left(c - d\sqrt{5}\right) = (a + c) - (b + d)\sqrt{5} = \overline{(a + b\sqrt{5})} + \overline{(c + d\sqrt{5})}$$

and that

$$\left(\overline{a + b\sqrt{5}}\right)\left(\overline{c + d\sqrt{5}}\right) = \left(a - b\sqrt{5}\right)\left(c - d\sqrt{5}\right) = (ac + 5bd) - (ad + bc)\sqrt{5} = \overline{(a + b\sqrt{5})}\left(\overline{c + d\sqrt{5}}\right).$$

Note that  $\overline{\varphi} = \psi$  and  $\overline{\psi} = \varphi$  by the  $(1 \pm \sqrt{5})/2$  formulas for  $\varphi$  and  $\psi$ .

Second, consider the  $p$ th power map that sends an element  $a + b\sqrt{5}$  to the  $p$ th power  $(a + b\sqrt{5})^p$ . This function clearly preserves multiplication. To see that this function preserves addition, note that the binomial coefficient  $\binom{p}{k}$  is divisible by  $p$  for  $1 \leq k \leq p - 1$ . This can be proved algebraically or by a rotation argument similar to the proof of Lemma 1. Then by the binomial formula,

$$(x + y)^p = \binom{p}{0}x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \dots + \binom{p}{p-2}x^2y^{p-2} + \binom{p}{p-1}xy^{p-1} + \binom{p}{p}y^p = x^p + y^p.$$

We summarize these results in the following proposition:



**Proposition 2.** *Let  $p$  be a prime such that  $\mathbb{F}_p$  does not contain a square root of 5. Then the conjugation map  $(a + b\sqrt{5}) \mapsto (a - b\sqrt{5})$  and the  $p$ th power map  $(a + b\sqrt{5}) \mapsto (a + b\sqrt{5})^p$  are automorphisms of  $\mathbb{F}_p(\sqrt{5})$ .*

The remarkable fact is that the two automorphisms in Proposition 2 are the same. This should be surprising because the two automorphisms arose in very different ways:

- The conjugation automorphism arose because our field was obtained by adding in a square root.
- The  $p$ th power automorphism arose because  $p = 0$  in our field.

As we will see in a later chapter, if  $K$  is a finite field in which  $p = 0$  then every automorphism of  $K$  is obtained by applying the  $p$ th power map some number of times (we would say that the automorphism group of  $K$  is cyclic and generated by the  $p$ th power map).

If we can show that  $5^{(p-1)/2} = -1$  in  $\mathbb{F}_p$  then Lemma 1 would give that

$$(a + b\sqrt{5})^p = a^p + 5^{\frac{p-1}{2}} b^p \sqrt{5} = a - b\sqrt{5} = \overline{a + b\sqrt{5}} \quad (1.7)$$

for all elements  $a + b\sqrt{5}$  of  $\mathbb{F}_p(\sqrt{5})$ . The result that  $5^{(p-1)/2} = -1$  in  $\mathbb{F}_p$  is an example of Euler's criterion:

**Lemma 2.** *Let  $p$  be an odd prime and let  $a$  be a nonzero element of  $\mathbb{F}_p$ . If  $\mathbb{F}_p$  has a square root of  $a$  then  $a^{(p-1)/2} = 1$  in  $\mathbb{F}_p$ . If  $\mathbb{F}_p$  does not have a square root of  $a$  then  $a^{(p-1)/2} = -1$  in  $\mathbb{F}_p$ .*

*Proof.* Suppose that  $\mathbb{F}_p$  does not have a square root of  $a$ . Then the  $p - 1$  nonzero elements of  $\mathbb{F}_p$  form  $(p - 1)/2$  pairs, each of which has product equal to  $a$  (pair  $b$  with  $a/b$ ). In particular, the product of the  $p - 1$  nonzero elements of  $\mathbb{F}_p$  is equal to  $a^{(p-1)/2}$ .

Suppose that  $\mathbb{F}_p$  has a square root of  $a$ . Let  $c$  and  $d$  be square roots of  $a$ . Now  $c^2 - d^2 = a - a = 0$  so  $(c - d)(c + d) = 0$ . Then either  $c = d$  or  $c = -d$ . This shows that  $c$  and  $-c$  are the only square roots of  $a$  (where  $c \neq -c$  since  $p \neq 2$ ). Then the  $p - 1$  nonzero elements of  $\mathbb{F}_p$  form  $(p - 1)/2$  pairs, each of which has product equal to  $a$  except for the  $\{c, -c\}$  pair which has product equal to  $-a$ . In particular, the product of the  $p - 1$  nonzero elements of  $\mathbb{F}_p$  is equal to  $-a^{(p-1)/2}$ . Since  $\mathbb{F}_p$  has a square root of 1, setting  $a = 1$  shows that the product of the  $p - 1$  nonzero elements of  $\mathbb{F}_p$  is also equal to  $-1$ .  $\square$

Lemma 2 shows that  $5^{(p-1)/2} = -1$  in  $\mathbb{F}_p$ . Then Equation 1.7 shows that the conjugation automorphism and the  $p$ th power automorphism are the same. Recall that  $\overline{\varphi} = \psi$  and  $\overline{\psi} = \varphi$  by the  $(1 \pm \sqrt{5})/2$  formulas for  $\varphi$  and  $\psi$ . Then Equation 1.7 gives that  $\varphi^p = \psi$  and  $\psi^p = \varphi$ . Consequently,  $\varphi^{p+1} = \varphi\psi = \psi^{p+1}$  so  $(\varphi/\psi)^{p+1} = 1$ . Then Theorem 2 proves the following corollary:

**Corollary 3.** *Let  $p \neq 2, 5$  be a prime and suppose that  $\mathbb{F}_p$  does not contain a square root of 5. Then  $F_{p+1}$  is divisible by  $p$ . Equivalently,  $a_p$  divides  $p + 1$ .*

## 1.8 Quadratic Reciprocity

For  $p = 2$ ,  $a_p = 3$  so every 3rd Fibonacci number is divisible by 2. For  $p = 5$ ,  $a_p = 5$  so every 5th Fibonacci number is divisible by 5. For a prime  $p \neq 2, 5$ , Corollaries 2 and 3 give information on when Fibonacci numbers are divisible by  $p$ . However, these corollaries require knowing whether or not  $\mathbb{F}_p$  contains a square root of 5. This question is answered by the law of quadratic reciprocity. Let  $p$  be an odd prime and let  $a$  be an integer not divisible by  $p$ . Define the Legendre symbol  $\left(\frac{a}{p}\right)$  to be  $+1$  if  $\mathbb{F}_p$  has a square root of  $a$  and to be  $-1$  if  $\mathbb{F}_p$  does not have a square root of  $a$ . We can now state the law of quadratic reciprocity.

**Theorem 3.** *For distinct odd primes  $p$  and  $q$ ,*

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$$

In the case that  $q = 5$ , Theorem 3 states that

$$\left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2} \frac{p-1}{2}} \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right) = \begin{cases} +1 & p \equiv 1, 4 \pmod{5} \\ -1 & p \equiv 2, 3 \pmod{5} \end{cases}.$$

The notation  $p \equiv a \pmod{5}$  means that  $p = a$  in  $\mathbb{F}_5$  ( $p$  and  $a$  have the same remainder when dividing by 5). Then Corollaries 2 and 3 prove the following result:

**Corollary 4.** *Let  $p$  be a prime.*

- *If  $p \equiv 1, 4 \pmod{5}$  then  $a_p$  divides  $p - 1$  and  $F_{p-1}$  is divisible by  $p$ .*
- *If  $p \equiv 2, 3 \pmod{5}$  then  $a_p$  divides  $p + 1$  and  $F_{p+1}$  is divisible by  $p$ .*
- *If  $p = 5$  then  $a_p = 5$  and every 5th Fibonacci number is divisible by 5.*

It remains to prove the law of quadratic reciprocity (Theorem 3). Unfortunately, this will be rather technical. For a positive integer  $n$ , let  $\mathbb{Z}/n\mathbb{Z}$  consist of the  $n$  distinct remainders when dividing modulo  $n$ , and let  $(\mathbb{Z}/n\mathbb{Z})^\times$  consist of the elements of  $\mathbb{Z}/n\mathbb{Z}$  that share no common factors with  $n$ . Consider the map  $\sigma: \mathbb{Z}/pq\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$  from remainders modulo  $pq$  to a pair consisting of a remainder modulo  $p$  and a remainder modulo  $q$ . If  $\sigma(x) = (0, 0)$  for some element  $x$  of  $\mathbb{Z}/pq\mathbb{Z}$  then  $x$  is divisible by both  $p$  and  $q$ . Then  $x$  is divisible by  $pq$  so  $x = 0$  (as an element of  $\mathbb{Z}/pq\mathbb{Z}$ ). If  $\sigma(x) = \sigma(y)$  then  $\sigma(x - y) = \sigma(x) - \sigma(y) = (0, 0)$  so  $x - y = 0$  and thus  $x = y$ . This shows that  $\sigma$  does not map different elements of  $\mathbb{Z}/pq\mathbb{Z}$  to the same element of  $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ . Since  $\mathbb{Z}/pq\mathbb{Z}$  and  $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$  have the same number of elements, this shows that  $\sigma$  is a bijection (a permutation or rearrangement). Restricting  $\sigma$  to  $(\mathbb{Z}/pq\mathbb{Z})^\times$  gives a bijection  $\sigma: (\mathbb{Z}/pq\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$ .

Now consider the following subsets of  $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$ :

$$S = \left\{ (x, y) \in (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times : 1 \leq x \leq \frac{p-1}{2} \right\}, \quad T = \left\{ \sigma(x) : x \in (\mathbb{Z}/pq\mathbb{Z})^\times \text{ and } 1 \leq x \leq \frac{pq-1}{2} \right\}.$$

Both  $S$  and  $T$  have the property that for all elements  $x$  of  $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$ , exactly one of  $x$  and  $-x$  is contained in the set. Then the products  $\prod S$  and  $\prod T$  differ only by a sign. Define  $P = (p-1)/2$  and  $Q = (q-1)/2$ . Then we have that

$$\prod S = (P!^{q-1}, (q-1)!^P) = ((p-1)!^Q (-1)^{PQ}, (q-1)!^P).$$

In  $(\mathbb{Z}/p\mathbb{Z})^\times$ , we have that

$$\prod T = \prod_{\substack{k < pq/2 \\ (k, pq) = 1}} k = \left( \prod_{\substack{k < pq/2 \\ p \nmid k}} k \right) \left( \prod_{\substack{k < pq/2 \\ q \nmid k}} k \right)^{-1} = \frac{(p-1)!^Q P!}{P! q^P} = (p-1)!^Q \left(\frac{q}{p}\right)$$

where the last equality follows from Lemma 2. Symmetrically, we have that

$$\prod T = \left( (p-1)!^Q \left(\frac{q}{p}\right), (q-1)!^P \left(\frac{p}{q}\right) \right).$$

Since  $\prod S$  and  $\prod T$  differ only by a sign, this shows that  $\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{PQ}$ .

## 1.9 An Example

We now apply Conjecture 1 and Corollary 4 to factor  $F_{37} = 24157817$  by hand. Let  $p$  be a prime dividing  $F_{37}$ . Since 37 is prime, Conjecture 1 implies that  $a_p = 37$ . If  $p \equiv 1, 4 \pmod{5}$  then Corollary 4 implies that  $p - 1$  is a multiple of 37. If  $p \equiv 2, 3 \pmod{5}$  then Corollary 4 implies that  $p + 1$  is a multiple of 37. The first few primes satisfying these conditions are

$$73, 149, 443, 887, 1259, 1481, 1553, 1627, 1997, 1999, 2221.$$

Checking the divisibility of  $F_{37}$  by these primes gives that  $F_{37} = 73 \cdot 149 \cdot 2221$ .

For another example, we factor  $F_{88} = 1100087778366101931$  by hand. First note that  $F_{88}$  is divisible by  $F_{44} = 3 \cdot 43 \cdot 89 \cdot 199 \cdot 307$  and by  $F_8 = 3 \cdot 7$ . Then  $F_{88}$  is divisible by  $3 \cdot 7 \cdot 43 \cdot 89 \cdot 199 \cdot 307$ . If  $p$  is any other prime dividing  $F_{88}$  then Conjecture 1 implies that  $a_p = 88$ . If  $p \equiv 1, 4 \pmod{5}$  then Corollary 4 implies that  $p - 1$  is a multiple of 88. If  $p \equiv 2, 3 \pmod{5}$  then Corollary 4 implies that  $p + 1$  is a multiple of 88. The first few primes satisfying these conditions are

$$89, 263, 881, 967.$$

Checking the divisibility of  $F_{88}$  by these primes gives that  $F_{88} = 3 \cdot 7 \cdot 43 \cdot 89 \cdot 199 \cdot 263 \cdot 307 \cdot 881 \cdot 967$ .

$F_1 = 1$	$F_{51} = 20365011074$	$F_{101} = 573147844013817084101$
$F_2 = 1$	$F_{52} = 32951280099$	$F_{102} = 927372692193078999176$
$F_3 = 2$	$F_{53} = 53316291173$	$F_{103} = 1500520536206896083277$
$F_4 = 3$	$F_{54} = 86267571272$	$F_{104} = 2427893228399975082453$
$F_5 = 5$	$F_{55} = 139583862445$	$F_{105} = 3928413764606871165730$
$F_6 = 8$	$F_{56} = 225851433717$	$F_{106} = 6356306993006846248183$
$F_7 = 13$	$F_{57} = 365435296162$	$F_{107} = 10284720757613717413913$
$F_8 = 21$	$F_{58} = 591286729879$	$F_{108} = 16641027750620563662096$
$F_9 = 34$	$F_{59} = 956722026041$	$F_{109} = 26925748508234281076009$
$F_{10} = 55$	$F_{60} = 1548008755920$	$F_{110} = 43566776258854844738105$
$F_{11} = 89$	$F_{61} = 2504730781961$	$F_{111} = 70492524767089125814114$
$F_{12} = 144$	$F_{62} = 4052739537881$	$F_{112} = 114059301025943970552219$
$F_{13} = 233$	$F_{63} = 6557470319842$	$F_{113} = 184551825793033096366333$
$F_{14} = 377$	$F_{64} = 10610209857723$	$F_{114} = 298611126818977066918552$
$F_{15} = 610$	$F_{65} = 17167680177565$	$F_{115} = 483162952612010163284885$
$F_{16} = 987$	$F_{66} = 27777890035288$	$F_{116} = 781774079430987230203437$
$F_{17} = 1597$	$F_{67} = 44945570212853$	$F_{117} = 1264937032042997393488322$
$F_{18} = 2584$	$F_{68} = 72723460248141$	$F_{118} = 2046711111473984623691759$
$F_{19} = 4181$	$F_{69} = 117669030460994$	$F_{119} = 3311648143516982017180081$
$F_{20} = 6765$	$F_{70} = 190392490709135$	$F_{120} = 5358359254990966640871840$
$F_{21} = 10946$	$F_{71} = 308061521170129$	$F_{121} = 8670007398507948658051921$
$F_{22} = 17711$	$F_{72} = 498454011879264$	$F_{122} = 14028366653498915298923761$
$F_{23} = 28657$	$F_{73} = 806515533049393$	$F_{123} = 22698374052006863956975682$
$F_{24} = 46368$	$F_{74} = 1304969544928657$	$F_{124} = 36726740705505779255899443$
$F_{25} = 75025$	$F_{75} = 2111485077978050$	$F_{125} = 59425114757512643212875125$
$F_{26} = 121393$	$F_{76} = 3416454622906707$	$F_{126} = 96151855463018422468774568$
$F_{27} = 196418$	$F_{77} = 5527939700884757$	$F_{127} = 155576970220531065681649693$
$F_{28} = 317811$	$F_{78} = 8944394323791464$	$F_{128} = 251728825683549488150424261$
$F_{29} = 514229$	$F_{79} = 14472334024676221$	$F_{129} = 407305795904080553832073954$
$F_{30} = 832040$	$F_{80} = 23416728348467685$	$F_{130} = 659034621587630041982498215$
$F_{31} = 1346269$	$F_{81} = 37889062373143906$	$F_{131} = 1066340417491710595814572169$
$F_{32} = 2178309$	$F_{82} = 61305790721611591$	$F_{132} = 1725375039079340637797070384$
$F_{33} = 3524578$	$F_{83} = 99194853094755497$	$F_{133} = 2791715456571051233611642553$
$F_{34} = 5702887$	$F_{84} = 160500643816367088$	$F_{134} = 4517090495650391871408712937$
$F_{35} = 9227465$	$F_{85} = 259695496911122585$	$F_{135} = 7308805952221443105020355490$
$F_{36} = 14930352$	$F_{86} = 420196140727489673$	$F_{136} = 11825896447871834976429068427$
$F_{37} = 24157817$	$F_{87} = 679891637638612258$	$F_{137} = 19134702400093278081449423917$
$F_{38} = 39088169$	$F_{88} = 1100087778366101931$	$F_{138} = 30960598847965113057878492344$
$F_{39} = 63245986$	$F_{89} = 1779979416004714189$	$F_{139} = 50095301248058391139327916261$
$F_{40} = 102334155$	$F_{90} = 2880067194370816120$	$F_{140} = 81055900096023504197206408605$
$F_{41} = 165580141$	$F_{91} = 4660046610375530309$	$F_{141} = 131151201344081895336534324866$
$F_{42} = 267914296$	$F_{92} = 7540113804746346429$	$F_{142} = 212207101440105399533740733471$
$F_{43} = 433494437$	$F_{93} = 12200160415121876738$	$F_{143} = 343358302784187294870275058337$
$F_{44} = 701408733$	$F_{94} = 19740274219868223167$	$F_{144} = 555565404224292694404015791808$
$F_{45} = 1134903170$	$F_{95} = 31940434634990099905$	$F_{145} = 898923707008479989274290850145$
$F_{46} = 1836311903$	$F_{96} = 51680708854858323072$	$F_{146} = 1454489111232772683678306641953$
$F_{47} = 2971215073$	$F_{97} = 83621143489848422977$	$F_{147} = 2353412818241252672952597492098$
$F_{48} = 4807526976$	$F_{98} = 135301852344706746049$	$F_{148} = 3807901929474025356630904134051$
$F_{49} = 7778742049$	$F_{99} = 218922995834555169026$	$F_{149} = 6161314747715278029583501626149$
$F_{50} = 12586269025$	$F_{100} = 354224848179261915075$	$F_{150} = 9969216677189303386214405760200$

Table 1: The first 150 Fibonacci numbers.

$F_1 = 1$	$F_{51} = 2 \cdot 1597 \cdot 6376021$
$F_2 = 1$	$F_{52} = 3 \cdot 233 \cdot 521 \cdot 90481$
$F_3 = 2$	$F_{53} = 953 \cdot 55945741$
$F_4 = 3$	$F_{54} = 2^3 \cdot 17 \cdot 19 \cdot 53 \cdot 109 \cdot 5779$
$F_5 = 5$	$F_{55} = 5 \cdot 89 \cdot 661 \cdot 474541$
$F_6 = 2^3$	$F_{56} = 3 \cdot 7^2 \cdot 13 \cdot 29 \cdot 281 \cdot 14503$
$F_7 = 13$	$F_{57} = 2 \cdot 37 \cdot 113 \cdot 797 \cdot 54833$
$F_8 = 3 \cdot 7$	$F_{58} = 59 \cdot 19489 \cdot 514229$
$F_9 = 2 \cdot 17$	$F_{59} = 353 \cdot 2710260697$
$F_{10} = 5 \cdot 11$	$F_{60} = 2^4 \cdot 3^2 \cdot 5 \cdot 11 \cdot 31 \cdot 41 \cdot 61 \cdot 2521$
$F_{11} = 89$	$F_{61} = 4513 \cdot 555003497$
$F_{12} = 2^4 \cdot 3^2$	$F_{62} = 557 \cdot 2417 \cdot 3010349$
$F_{13} = 233$	$F_{63} = 2 \cdot 13 \cdot 17 \cdot 421 \cdot 35239681$
$F_{14} = 13 \cdot 29$	$F_{64} = 3 \cdot 7 \cdot 47 \cdot 1087 \cdot 2207 \cdot 4481$
$F_{15} = 2 \cdot 5 \cdot 61$	$F_{65} = 5 \cdot 233 \cdot 14736206161$
$F_{16} = 3 \cdot 7 \cdot 47$	$F_{66} = 2^3 \cdot 89 \cdot 199 \cdot 9901 \cdot 19801$
$F_{17} = 1597$	$F_{67} = 269 \cdot 116849 \cdot 1429913$
$F_{18} = 2^3 \cdot 17 \cdot 19$	$F_{68} = 3 \cdot 67 \cdot 1597 \cdot 3571 \cdot 63443$
$F_{19} = 37 \cdot 113$	$F_{69} = 2 \cdot 137 \cdot 829 \cdot 18077 \cdot 28657$
$F_{20} = 3 \cdot 5 \cdot 11 \cdot 41$	$F_{70} = 5 \cdot 11 \cdot 13 \cdot 29 \cdot 71 \cdot 911 \cdot 141961$
$F_{21} = 2 \cdot 13 \cdot 421$	$F_{71} = 6673 \cdot 46165371073$
$F_{22} = 89 \cdot 199$	$F_{72} = 2^5 \cdot 3^3 \cdot 7 \cdot 17 \cdot 19 \cdot 23 \cdot 107 \cdot 103681$
$F_{23} = 28657$	$F_{73} = 9375829 \cdot 86020717$
$F_{24} = 2^5 \cdot 3^2 \cdot 7 \cdot 23$	$F_{74} = 73 \cdot 149 \cdot 2221 \cdot 54018521$
$F_{25} = 5^2 \cdot 3001$	$F_{75} = 2 \cdot 5^2 \cdot 61 \cdot 3001 \cdot 230686501$
$F_{26} = 233 \cdot 521$	$F_{76} = 3 \cdot 37 \cdot 113 \cdot 9349 \cdot 29134601$
$F_{27} = 2 \cdot 17 \cdot 53 \cdot 109$	$F_{77} = 13 \cdot 89 \cdot 988681 \cdot 4832521$
$F_{28} = 3 \cdot 13 \cdot 29 \cdot 281$	$F_{78} = 2^3 \cdot 79 \cdot 233 \cdot 521 \cdot 859 \cdot 135721$
$F_{29} = 514229$	$F_{79} = 157 \cdot 92180471494753$
$F_{30} = 2^3 \cdot 5 \cdot 11 \cdot 31 \cdot 61$	$F_{80} = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 41 \cdot 47 \cdot 1601 \cdot 2161 \cdot 3041$
$F_{31} = 557 \cdot 2417$	$F_{81} = 2 \cdot 17 \cdot 53 \cdot 109 \cdot 2269 \cdot 4373 \cdot 19441$
$F_{32} = 3 \cdot 7 \cdot 47 \cdot 2207$	$F_{82} = 2789 \cdot 59369 \cdot 370248451$
$F_{33} = 2 \cdot 89 \cdot 19801$	$F_{83} = 99194853094755497$
$F_{34} = 1597 \cdot 3571$	$F_{84} = 2^4 \cdot 3^2 \cdot 13 \cdot 29 \cdot 83 \cdot 211 \cdot 281 \cdot 421 \cdot 1427$
$F_{35} = 5 \cdot 13 \cdot 141961$	$F_{85} = 5 \cdot 1597 \cdot 9521 \cdot 3415914041$
$F_{36} = 2^4 \cdot 3^3 \cdot 17 \cdot 19 \cdot 107$	$F_{86} = 6709 \cdot 144481 \cdot 433494437$
$F_{37} = 73 \cdot 149 \cdot 2221$	$F_{87} = 2 \cdot 173 \cdot 514229 \cdot 3821263937$
$F_{38} = 37 \cdot 113 \cdot 9349$	$F_{88} = 3 \cdot 7 \cdot 43 \cdot 89 \cdot 199 \cdot 263 \cdot 307 \cdot 881 \cdot 967$
$F_{39} = 2 \cdot 233 \cdot 135721$	$F_{89} = 1069 \cdot 1665088321800481$
$F_{40} = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 41 \cdot 2161$	$F_{90} = 2^3 \cdot 5 \cdot 11 \cdot 17 \cdot 19 \cdot 31 \cdot 61 \cdot 181 \cdot 541 \cdot 109441$
$F_{41} = 2789 \cdot 59369$	$F_{91} = 13^2 \cdot 233 \cdot 741469 \cdot 159607993$
$F_{42} = 2^3 \cdot 13 \cdot 29 \cdot 211 \cdot 421$	$F_{92} = 3 \cdot 139 \cdot 461 \cdot 4969 \cdot 28657 \cdot 275449$
$F_{43} = 433494437$	$F_{93} = 2 \cdot 557 \cdot 2417 \cdot 4531100550901$
$F_{44} = 3 \cdot 43 \cdot 89 \cdot 199 \cdot 307$	$F_{94} = 2971215073 \cdot 6643838879$
$F_{45} = 2 \cdot 5 \cdot 17 \cdot 61 \cdot 109441$	$F_{95} = 5 \cdot 37 \cdot 113 \cdot 761 \cdot 29641 \cdot 67735001$
$F_{46} = 139 \cdot 461 \cdot 28657$	$F_{96} = 2^7 \cdot 3^2 \cdot 7 \cdot 23 \cdot 47 \cdot 769 \cdot 1103 \cdot 2207 \cdot 3167$
$F_{47} = 2971215073$	$F_{97} = 193 \cdot 389 \cdot 3084989 \cdot 361040209$
$F_{48} = 2^6 \cdot 3^2 \cdot 7 \cdot 23 \cdot 47 \cdot 1103$	$F_{98} = 13 \cdot 29 \cdot 97 \cdot 6168709 \cdot 599786069$
$F_{49} = 13 \cdot 97 \cdot 6168709$	$F_{99} = 2 \cdot 17 \cdot 89 \cdot 197 \cdot 19801 \cdot 18546805133$
$F_{50} = 5^2 \cdot 11 \cdot 101 \cdot 151 \cdot 3001$	$F_{100} = 3 \cdot 5^2 \cdot 11 \cdot 41 \cdot 101 \cdot 151 \cdot 401 \cdot 3001 \cdot 570601$

Table 2: The factorizations of the first 100 Fibonacci numbers.

$a_2 = 3$	$a_{2^2} = 6$	$a_{2^3} = 6$	$a_{2^4} = 12$	$a_{2^5} = 24$
$a_3 = 4$	$a_{3^2} = 12$	$a_{3^3} = 36$	$a_{3^4} = 108$	$a_{3^5} = 324$
$a_5 = 5$	$a_{5^2} = 25$	$a_{5^3} = 125$	$a_{5^4} = 625$	$a_{5^5} = 3125$
$a_7 = 8$	$a_{7^2} = 56$	$a_{7^3} = 392$	$a_{7^4} = 2744$	$a_{7^5} = 19208$
$a_{11} = 10$	$a_{11^2} = 110$	$a_{11^3} = 1210$	$a_{11^4} = 13310$	$a_{11^5} = 146410$
$a_{13} = 7$	$a_{13^2} = 91$	$a_{13^3} = 1183$	$a_{13^4} = 15379$	$a_{13^5} = 199927$
$a_{17} = 9$	$a_{17^2} = 153$	$a_{17^3} = 2601$	$a_{17^4} = 44217$	$a_{17^5} = 751689$
$a_{19} = 18$	$a_{19^2} = 342$	$a_{19^3} = 6498$	$a_{19^4} = 123462$	$a_{19^5} = 2345778$
$a_{23} = 24$	$a_{23^2} = 552$	$a_{23^3} = 12696$	$a_{23^4} = 292008$	$a_{23^5} = 6716184$
$a_{29} = 14$	$a_{29^2} = 406$	$a_{29^3} = 11774$	$a_{29^4} = 341446$	$a_{29^5} = 9901934$
$a_{31} = 30$	$a_{31^2} = 930$	$a_{31^3} = 28830$	$a_{31^4} = 893730$	$a_{31^5} = 27705630$
$a_{37} = 19$	$a_{37^2} = 703$	$a_{37^3} = 26011$	$a_{37^4} = 962407$	$a_{37^5} = 35609059$
$a_{41} = 20$	$a_{41^2} = 820$	$a_{41^3} = 33620$	$a_{41^4} = 1378420$	$a_{41^5} = 56515220$
$a_{43} = 44$	$a_{43^2} = 1892$	$a_{43^3} = 81356$	$a_{43^4} = 3498308$	$a_{43^5} = 150427244$
$a_{47} = 16$	$a_{47^2} = 752$	$a_{47^3} = 35344$	$a_{47^4} = 1661168$	$a_{47^5} = 78074896$
$a_{53} = 27$	$a_{53^2} = 1431$	$a_{53^3} = 75843$	$a_{53^4} = 4019679$	$a_{53^5} = 213042987$
$a_{59} = 58$	$a_{59^2} = 3422$	$a_{59^3} = 201898$	$a_{59^4} = 11911982$	$a_{59^5} = 702806938$
$a_{61} = 15$	$a_{61^2} = 915$	$a_{61^3} = 55815$	$a_{61^4} = 3404715$	$a_{61^5} = 207687615$
$a_{67} = 68$	$a_{67^2} = 4556$	$a_{67^3} = 305252$	$a_{67^4} = 20451884$	$a_{67^5} = 1370276228$
$a_{71} = 70$	$a_{71^2} = 4970$	$a_{71^3} = 352870$	$a_{71^4} = 25053770$	$a_{71^5} = 1778817670$
$a_{73} = 37$	$a_{73^2} = 2701$	$a_{73^3} = 197173$	$a_{73^4} = 14393629$	$a_{73^5} = 1050734917$
$a_{79} = 78$	$a_{79^2} = 6162$	$a_{79^3} = 486798$	$a_{79^4} = 38457042$	$a_{79^5} = 3038106318$
$a_{83} = 84$	$a_{83^2} = 6972$	$a_{83^3} = 578676$	$a_{83^4} = 48030108$	$a_{83^5} = 3986498964$
$a_{89} = 11$	$a_{89^2} = 979$	$a_{89^3} = 87131$	$a_{89^4} = 7754659$	$a_{89^5} = 690164651$
$a_{97} = 49$	$a_{97^2} = 4753$	$a_{97^3} = 461041$	$a_{97^4} = 44720977$	$a_{97^5} = 4337934769$
$a_{101} = 50$	$a_{101^2} = 5050$	$a_{101^3} = 510050$	$a_{101^4} = 51515050$	$a_{101^5} = 5203020050$
$a_{103} = 104$	$a_{103^2} = 10712$	$a_{103^3} = 1103336$	$a_{103^4} = 113643608$	$a_{103^5} = 11705291624$
$a_{107} = 36$	$a_{107^2} = 3852$	$a_{107^3} = 412164$	$a_{107^4} = 44101548$	$a_{107^5} = 4718865636$
$a_{109} = 27$	$a_{109^2} = 2943$	$a_{109^3} = 320787$	$a_{109^4} = 34965783$	$a_{109^5} = 3811270347$
$a_{113} = 19$	$a_{113^2} = 2147$	$a_{113^3} = 242611$	$a_{113^4} = 27415043$	$a_{113^5} = 3097899859$
$a_{127} = 128$	$a_{127^2} = 16256$	$a_{127^3} = 2064512$	$a_{127^4} = 262193024$	$a_{127^5} = 33298514048$
$a_{131} = 130$	$a_{131^2} = 17030$	$a_{131^3} = 2230930$	$a_{131^4} = 292251830$	$a_{131^5} = 38284989730$
$a_{137} = 69$	$a_{137^2} = 9453$	$a_{137^3} = 1295061$	$a_{137^4} = 177423357$	$a_{137^5} = 24306999909$
$a_{139} = 46$	$a_{139^2} = 6394$	$a_{139^3} = 888766$	$a_{139^4} = 123538474$	$a_{139^5} = 17171847886$
$a_{149} = 37$	$a_{149^2} = 5513$	$a_{149^3} = 821437$	$a_{149^4} = 122394113$	$a_{149^5} = 18236722837$
$a_{151} = 50$	$a_{151^2} = 7550$	$a_{151^3} = 1140050$	$a_{151^4} = 172147550$	$a_{151^5} = 25994280050$
$a_{157} = 79$	$a_{157^2} = 12403$	$a_{157^3} = 1947271$	$a_{157^4} = 305721547$	$a_{157^5} = 47998282879$
$a_{163} = 164$	$a_{163^2} = 26732$	$a_{163^3} = 4357316$	$a_{163^4} = 710242508$	$a_{163^5} = 115769528804$
$a_{167} = 168$	$a_{167^2} = 28056$	$a_{167^3} = 4685352$	$a_{167^4} = 782453784$	$a_{167^5} = 130669781928$
$a_{173} = 87$	$a_{173^2} = 15051$	$a_{173^3} = 2603823$	$a_{173^4} = 450461379$	$a_{173^5} = 77929818567$
$a_{179} = 178$	$a_{179^2} = 31862$	$a_{179^3} = 5703298$	$a_{179^4} = 1020890342$	$a_{179^5} = 182739371218$
$a_{181} = 90$	$a_{181^2} = 16290$	$a_{181^3} = 2948490$	$a_{181^4} = 533676690$	$a_{181^5} = 96595480890$
$a_{191} = 190$	$a_{191^2} = 36290$	$a_{191^3} = 6931390$	$a_{191^4} = 1323895490$	$a_{191^5} = 252864038590$
$a_{193} = 97$	$a_{193^2} = 18721$	$a_{193^3} = 3613153$	$a_{193^4} = 697338529$	$a_{193^5} = 134586336097$
$a_{197} = 99$	$a_{197^2} = 19503$	$a_{197^3} = 3842091$	$a_{197^4} = 756891927$	$a_{197^5} = 149107709619$
$a_{199} = 22$	$a_{199^2} = 4378$	$a_{199^3} = 871222$	$a_{199^4} = 173373178$	$a_{199^5} = 34501262422$
$a_{211} = 42$	$a_{211^2} = 8862$	$a_{211^3} = 1869882$	$a_{211^4} = 394545102$	$a_{211^5} = 83249016522$
$a_{223} = 224$	$a_{223^2} = 49952$	$a_{223^3} = 11139296$	$a_{223^4} = 2484063008$	$a_{223^5} = 553946050784$
$a_{227} = 228$	$a_{227^2} = 51756$	$a_{227^3} = 11748612$	$a_{227^4} = 2666934924$	$a_{227^5} = 605394227748$
$a_{229} = 114$	$a_{229^2} = 26106$	$a_{229^3} = 5978274$	$a_{229^4} = 1369024746$	$a_{229^5} = 313506666834$

Table 3: The values of  $a_{p^b}$  for primes  $p \leq 230$  and integers  $1 \leq b \leq 5$ .