

Tutorial 2

1. For each natural number n , let a_n be the residue of 2^n modulo 13. Since $a_{k+1} \equiv 2a_k \pmod{13}$ for each $k \in \mathbb{N}$, it follows that the a_k are easy to compute recursively, starting at $a_0 = 1$ and then doubling and reducing mod 13 to get successive terms of the sequence. Compute the first dozen or so terms, and then compute a_{2010} .

Solution.

1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1 – and then it repeats. In other words, $a_0 = a_{12} = a_{24} = \dots$, and $a_1 = a_{13} = a_{25} = \dots$, etc. In general, $a_i = a_j$ if and only if $i \equiv j \pmod{12}$. (In the terminology introduced in lectures, $\text{ord}_{13}(2) = 12$.) Now $2010 \equiv 6 \pmod{12}$; so $a_{2010} = a_6 = 12$.

2. Compute the residue of $2^{2010} \pmod{p}$, for each $p \in \{3, 5, 7, 11, 31, 47\}$.

Solution.

For 3 the sequence of residues of $2^i \pmod{p}$ is just 1, 2, 1, 2, ...; that is, $a_i = 1$ if i is even and $a_i = 2$ if i is odd (and $\text{ord}_3(2) = 2$). So $a_{2010} = 1$.

Using 5 we get 1, 2, 4, 3, 1, ... So $\text{ord}_5(2) = 4$, and $a_{2010} = a_2 = 4$ (since $2009 \equiv 1 \pmod{4}$).

Using 7 we get 1, 2, 4, 1, ... So $\text{ord}_7(2) = 3$, and $a_{2010} = a_0 = 1$ (since $2009 \equiv 2 \pmod{3}$).

Using 11 we get 1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1, ... So $\text{ord}_{11}(2) = 10$, and $a_{2010} = a_0 = 1$ (since $2010 \equiv 0 \pmod{10}$).

Using 31 we get 1, 2, 4, 8, 16, 1, ... So $\text{ord}_{31}(2) = 5$, and $a_{2010} = a_0 = 1$ (since $2010 \equiv 0 \pmod{5}$).

Using 47 we get 1, 2, 4, 8, 16, 32, 17, 34, 21, 42, 37, 27, 7, 14, 28, 9, 18, 36, 25, 3, 6, 12, 24, 1, ... So $\text{ord}_{47}(2) = 23$, and $a_{2010} = a_9 = 42$ (since $2010 \equiv 9 \pmod{23}$).

Observe that in all these case, $\text{ord}_p(2)$ is a divisor of $p - 1$.

3. Let p be a prime. The mod p Fibonacci sequence is the sequence a_0, a_1, a_2, \dots defined as follows: $a_0 = 0, a_1 = 1$, and for all $i \geq 2$, a_i is the residue of $a_{i-2} + a_{i-1} \pmod{p}$. Compute the first few terms in the case $p = 7$. Then compute a_{2010} . Repeat this for other primes less than 20.

Solution.

The mod 7 Fibonacci sequence goes 0, 1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, 1, ... Since $a_{16} = a_0$ and $a_{17} = a_1$ it follows that $a_{18} = a_3$, then $a_{19} = a_4$, then $a_{20} = a_5$, and so on. The sequence is periodic with period 16. Since $2010 \equiv 10 \pmod{16}$ it follows that $a_{2010} = a_{10} = 6$.

Modulo 2 the Fibonacci sequence goes 0, 1, 1, 0, 1, 1, 0, ... So $a_i = 0$ if i is a multiple of 3, and $a_i = 1$ otherwise. So $a_{2010} = 0$.

Modulo 3 we get 0, 1, 1, 2, 0, 2, 2, 1, 0, after which it repeats. So $a_i \equiv a_j \pmod{3}$ whenever $i \equiv j \pmod{8}$. Thus $a_{2010} = a_2 = 1$.

Modulo 5 we get 0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, after which it repeats. So $a_i \equiv a_j \pmod{5}$ whenever $i \equiv j \pmod{20}$. Thus $a_{2010} = a_{10} = 0$.

Modulo 11 we get 0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0 and repetition. So $a_i \equiv a_j \pmod{11}$ whenever $i \equiv j \pmod{10}$. Thus $a_{2010} = a_0 = 0$.

Modulo 13 we get 0, 1, 1, 2, 3, 5, 8, 0, 8, 8, 3, 11, 1, 12, 0, 12, 12, 11, 10, 8, 5, 0, 5, 5, 10, 2, 12, 1, 0 and repetition. So $a_i \equiv a_j \pmod{13}$ whenever $i \equiv j \pmod{28}$. Thus $a_{2010} = a_{22} = 5$.

Modulo 17 we get 0, 1, 1, 2, 3, 5, 8, 13, 4, 0, 4, 4, 8, 12, 3, 15, 1, 16, 0, 16, 16, 15, 14, 12, 9, 4, 13, 0, 13, 13, 9, 5, 14, 2, 16, 1, 0 and repetition. So $a_i \equiv a_j \pmod{17}$ whenever $i \equiv j \pmod{36}$. Thus $a_{2010} = a_{30} = 9$.

The period is $p + 1$ when $p = 2$, $2(p + 1)$ when $p = 3, 13$ or 17 , $p - 1$ when $p = 11$, and takes the rather exceptional value $4p$ when $p = 5$. In order to understand the periodicity better, it helps to look at the first $i > 0$ such that $a_i = 0$. The period is always a multiple of this. And it turns out that this i is always a divisor of $p + 1$ or $p - 1$, except when the prime p is 5.

4. (i) Compute $n^2 + n + 41$ for all values of n from 0 to 10, and check that in each case the answer is prime.
 (ii) Write down a value of n for which $n^2 + n + 41$ is *obviously* not prime. (Do **not** do any calculation).

Solution.

41, 43, 47, 53, 61, 71, 83, 97, 113, 131 and 151 are all prime. But why stop here! Going on with $n = 11, 12$ etc. we get 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523 and 1601, all of which are prime. The next value, corresponding to $n = 40$, is 1681, which is not prime. Indeed, $1681 = 41^2$, and it is reasonably obvious that $40^2 + 40 + 41 = 41^2$. It is even more obvious that $41^2 + 41 + 41$ is not prime, being divisible by 41. (But it is remarkable that it worked for as long as it did!)

5. (i) We saw in Tutorial 1 that if b is a factor of a then $2^b - 1$ is a factor of $2^a - 1$. So $2^a - 1$ is not prime if a is not prime. Check that $2^a - 1$ is prime for the first

four primes (2, 3, 5 and 7), but not for 11. (If a is prime then $2^a - 1$ is called a *Mersenne number*.)

- (ii) Show that $2^a + 1$ is divisible by 3 if a is odd, and by 5 if a is twice an odd number. More generally, show that $2^a + 1$ is not prime if a divisible by an odd number greater than 1.
- (iii) Deduce from Part (ii) that if $2^a + 1$ is prime then a is a power of 2. And check that $2^a + 1$ is indeed prime for $a = 0, 1, 2, 4, 8$.

Solution.

- (i) $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$ and $2^7 - 1 = 127$ are prime. But $2^{11} - 1 = 23 \times 89$. The largest known prime is a Mersenne prime. (As we shall see in due course, any divisor of $2^p - 1$, where p is prime, must have the form $kp + 1$ for some k ; this fact makes it easier to check whether or not $2^p - 1$ is prime than it is to check other odd numbers of similar size.)
- (ii) If k is odd then $x = -1$ is a solution of the polynomial equation $x^k + 1 = 0$. This tells us that $x^k + 1 = (x + 1)q(x)$ for some polynomial $q(x)$. In fact it is easy to check that $x^k + 1 = (x + 1)(x^{k-1} - x^{k-2} + x^{k-3} - \dots + x^2 - x + 1)$. (Notice that $1 - x + x^2 - x^3 + \dots - x^{k-2} + x^{k-1}$ is a geometric series with first term 1 and common ratio $-x$; so the formula for the sum of a geometric series tells you that it equals $(1 - (-x)^k)/(1 - (-x)) = (1 + x^k)/(1 + x)$.) Now putting $x = 2^b$ gives $2^{bk} + 1 = (2^b + 1)(2^{(k-1)b} - 2^{(k-2)b} + \dots + 2^{2b} - 2^b + 1)$. When $b = 1$ this shows that $2^k + 1$ is divisible by $2 + 1 = 3$, and when $b = 2$ it shows that $2^{2b} + 1$ is divisible by $2^2 + 1 = 5$. And in general, if $a = bk$, where k is odd and greater than 1, then $2^a + 1$ is divisible by $2^b + 1$. Observe that $2^b + 1$ is greater than 1 (since b is a positive integer) and less than $2^a + 1$ (since $b < a$).
- (iii) If $a > 1$ is not a power of 2 then (at least) one of the prime factors of a must be odd. So a is divisible by some odd number k . Writing $a = bk$, as above, we see that $2^a + 1$ is divisible by $2^b + 1$, and hence $2^a + 1$ is not prime. So when $2^a + 1$ is prime, a must be a power of 2. The first few powers of 2 are 1, 2, 4, 8 and 16, and we find that $2^1 + 1 = 3$, $2^2 + 1 = 5$, $2^4 + 1 = 17$, $2^8 + 1 = 257$ and $2^{16} + 1 = 65537$ are prime. But $2^{32} + 1$ is divisible by 641 – see the next question.

6. Observe that $641 = 5 \times 128 + 1 = 5 \times 2^7 + 1$. So $5 \times 2^7 \equiv -1 \pmod{641}$. Observe also that $641 = 625 + 16 = 5^4 + 2^4$; so $5^4 \equiv -2^4 \pmod{641}$. Use these facts to prove that $2^{32} \equiv -1 \pmod{641}$ (and hence $2^{32} + 1$ is not prime).

Solution.

Since $5 \times 2^7 \equiv -1 \pmod{641}$, it follows that

$$5^4 \times 2^{28} = (5 \times 2^7)^4 \equiv (-1)^4 \pmod{641}.$$

That is, $5^4 \times 2^{28} \equiv 1 \pmod{641}$. But now $5^4 \equiv -2^4 \pmod{641}$; so

$$1 \equiv 5^4 \times 2^{28} \equiv -2^4 \times 2^{28} = -2^{32} \pmod{641},$$

whence $2^{32} + 1 \equiv 0 \pmod{641}$. This shows that $641 \mid 2^{32} + 1$.

- *7. Let p be a prime and q a prime divisor of $2^p - 1$. Use Fermat's Little Theorem to prove that $q \equiv 1 \pmod{p}$. (Hint: Consider $\text{ord}_q(2)$.) Similarly prove that if r is a prime factor of $2^{2^k} + 1$ then $r \equiv 1 \pmod{2^{k+1}}$.

Solution.

Let a_n be the residue of $2^n \pmod{q}$. We know that the sequence a_0, a_1, a_2, \dots is periodic with period $m = \text{ord}_q(2)$. So $a_n = 1$ if and only if $m \mid n$. Since q is a divisor of $2^p - 1$ it follows that $2^p \equiv 1 \pmod{q}$; so $a_p = 1$. So $m \mid p$. But p is prime, and certainly $m \neq 1$ since $a_1 = 2 \not\equiv 1 \pmod{q}$. So $m = p$. But $2^{q-1} \equiv 1 \pmod{q}$ by Fermat; so $a_{q-1} = 1$ and so $m \mid (q-1)$. That is, $p \mid (q-1)$, which can be re-expressed as $q \equiv 1 \pmod{p}$.

If $r \mid (2^{2^k} + 1)$ then $2^{2^k} \equiv -1 \pmod{r}$ and so $2^{2^{k+1}} = (2^{2^k})^2 \equiv 1 \pmod{r}$. So $\text{ord}_r(2)$ is a divisor of 2^{k+1} , which certainly means that $\text{ord}_r(2)$ is a power of 2 less than or equal to 2^{k+1} . But $2^{2^k} \not\equiv 1 \pmod{r}$; so $\text{ord}_r(2)$ is not a divisor of 2^k . The only divisor of 2^{k+1} that is not a divisor of 2^k is 2^{k+1} itself. So $\text{ord}_r(2) = 2^{k+1}$. But Fermat says that $\text{ord}_r(2)$ is a divisor of $r-1$; so $r \equiv 1 \pmod{2^{k+1}}$.

- *8. In Tutorial 1 we factorized 10875593 by finding numbers k such that all the prime factors of $k^2 - 10875593$ were less than 20. Find three primes less than 20 that can never occur as factors of numbers of the form $k^2 - 10875593$.

Solution.

Firstly, 3 cannot occur. If $3 \mid (k^2 - 10875593)$ then $k^2 \equiv 10875593 \equiv 2 \pmod{3}$. But if $k \equiv 1 \pmod{3}$ then $k^2 \equiv 1^2 = 1$ and if $k \equiv 2 \pmod{3}$ then $k^2 \equiv 2^2 \equiv 1$, while if $k \equiv 0 \pmod{3}$ then $k^2 \equiv 0$. You can never get $k^2 \equiv 2 \pmod{3}$.

Similarly, 5 cannot occur. Every integer k must be congruent mod 5 to 0 or to ± 1 or to ± 2 , giving k^2 congruent to 0 or to 1 or to 4. It is impossible to have $k^2 \equiv 10875593 \equiv 3 \pmod{5}$.

The other one is 19. We find that $10875593 \equiv 12 \pmod{19}$, and squaring $\pm k$ for all natural numbers $k \leq 9$ we find that $k^2 \equiv 12 \pmod{19}$ never occurs.

- *9. A probability space on n outcomes is a sequence of n nonnegative numbers that sum to 1. The coincidence index is the probability that two independent performances of the associated experiment will produce the same outcome. Use the Cauchy-Schwarz inequality to show that the CI is minimized when all outcomes are equiprobable.

Solution.

Regard the probability space as an n -component vector $\mathbf{v} = (p_1, p_2, \dots, p_n)$. Note that the CI is $C = \sum_{i=1}^n p_i^2 = \|\mathbf{v}\|^2$. Let $\mathbf{u} = (1, 1, \dots, 1)$. Then $\mathbf{u} \cdot \mathbf{v} = \sum_{i=1}^n p_i = 1$, and $\|\mathbf{u}\| \|\mathbf{v}\| = \sqrt{n} \sqrt{C}$. So the Cauchy-Schwarz Inequality tells us that $\sqrt{n} \sqrt{C} \geq 1$ with equality if and only if \mathbf{v} is a scalar multiple of \mathbf{u} . So the minimum value of the CI is $1/n$, occurring when the p_i all equal $1/n$.