

### Tutorial 2

1. For each natural number  $n$ , let  $a_n$  be the residue of  $2^n$  modulo 13. Observe that  $a_{k+1} \equiv 2a_k \pmod{13}$  for each  $k \in \mathbb{N}$ ; hence 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  $a_{2009}$ .
2. Compute the residue of  $2^{2009} \pmod{p}$ , for each  $p \in \{3, 5, 7, 11, 31, 47\}$ .
3. Let  $p$  be a prime number. 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  $a_{2009}$ . Repeat this for other primes less than 20.
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).
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  $a = 0, 1, 2, 4, 8$ .
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).
- \*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  $r \equiv 1 \pmod{2^{k+1}}$ .
- \*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 such numbers.