

Math 104A, Practice Final, Fall 2002.

All numbers are assumed to be integers unless otherwise stated.

1. The Fibonacci numbers f_k are defined by $f_0 = 0$, $f_1 = 1$ and $f_{k+1} = f_k + f_{k-1}$. Show by induction on d that for $d \geq 0$ and $k \geq 0$,

$$f_{k+d+1} = f_{k+1}f_{d+1} + f_k f_d.$$

Solution. Fix k and let

$$S = \{d : f_{k+d+1} = f_{k+1}f_{d+1} + f_k f_d\}.$$

We wish to show that $S = \mathbb{N}$. First note that because $f_1 = 1$ and $f_0 = 0$ we do indeed have $f_{k+1} = f_{k+1}f_1 + f_k f_0$ so $0 \in S$. Furthermore $f_2 = f_1 = 1$ and so $f_{k+2} = f_{k+1} + f_k = f_{k+1}f_2 + f_k f_1$ and so $1 \in S$. Now suppose that the values $0, 1, \dots, d-1$ are in S . We must show that $d \in S$. We have

$$\begin{aligned} f_{k+d+1} &= f_{k+d} + f_{k+d-1} && \text{(from the definition of Fibonacci numbers)} \\ &= (f_{k+1}f_d + f_k f_{d-1}) + (f_{k+1}f_{d-1} + f_k f_{d-2}) && \text{(by the induction hypothesis)} \\ &= f_{k+1}(f_d + f_{d-1}) + f_k(f_{d-1} + f_{d-2}) \\ &= f_{k+1}f_{d+1} + f_k f_d && \text{(from the definition of Fibonacci numbers).} \end{aligned}$$

Hence $d \in S$, and by the extended induction principle $S = \mathbb{N}$.

2. Write down the general solution (x, y) of the equation $7x + 8y = 50$, and determine all solutions with x and y both positive.

Solution. Note that $1 = 8 - 7$ so $50 = 7 \cdot (-50) + 8 \cdot 50$ and $(x_0, y_0) = (-50, 50)$ is a solution. The general solution is given by $(x, y) = (-50 + 8k, 50 - 7k)$. For x and y to be positive we need $-50 + 8k > 0$ and $50 - 7k > 0$. These conditions give

$$\frac{50}{8} < k < \frac{50}{7}.$$

Since $6 < 50/8 < 7$ and $7 < 50/7 < 8$ we find that the only solution is $k = 7$. Then $(x, y) = (-50 + 56, 50 - 49) = (6, 1)$.

3. If s and t are positive and relatively prime and r_k is the remainder when ks is divided by t , then

$$r_0 + \cdots + r_{t-1} = at^2 + bt + c.$$

What are the rational numbers a , b and c ? Explain.

We claim that the numbers r_0, r_1, \dots, r_{t-1} are just the numbers $0, 1, \dots, t-1$ possibly in some other order. Hence

$$r_0 + \dots + r_{t-1} = 0 + 1 + \dots + (t-1) = \frac{1}{2}t(t-1) = \frac{t^2}{2} - \frac{t}{2},$$

so $a = 1/2$, $b = -1/2$ and $c = 0$.

To prove the claim, note first that $0 \leq r_\ell < t$ for every ℓ . We will show that r_0, r_1, \dots, r_{t-1} are all different, and so they must be all the values $0, 1, \dots, (t-1)$. Suppose that $r_\ell = r_m$. Then ℓs has the same remainder as $m s$ when divided by t and so $t | (\ell - m)s = 0$. Since $(s, t) = 1$, this implies $t | (\ell - m)$. But since $|\ell - m| < t$ this implies $\ell = m$. This proves that r_0, r_1, \dots, r_{t-1} are all different.

4. List the numbers a with $0 \leq a < 20$ such that there is at least one solution x to the equation

$$ax \equiv 14 \pmod{20}.$$

Solution. There exists at least one solution precisely when $(a, 20) | 14$.

a	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$(a, 20)$	20	1	2	1	4	5	2	1	4	1	10	1	4	1	2	5	4	1	2	1

The possible values of a are 1, 2, 3, 6, 7, 9, 11, 13, 14, 17, 18, 19.

5. Decide which of the following statements are true for every integer x , and all positive integers c and m , and justify your answer.

- (i) $cx \equiv 0 \pmod{cm} \Rightarrow x \equiv 0 \pmod{m}$.
- (ii) $x \equiv 0 \pmod{m} \Rightarrow cx \equiv 0 \pmod{cm}$.
- (iii) $cx \equiv 0 \pmod{cm} \Rightarrow x \equiv 0 \pmod{cm}$.
- (iv) $x \equiv 0 \pmod{cm} \Rightarrow x \equiv 0 \pmod{m}$.

(i) is true.

$$\begin{aligned} cx \equiv 0 \pmod{cm} &\Rightarrow cm | cx \Rightarrow \text{there exists } y \text{ with } cmy = cx \\ &\Rightarrow my = x \Rightarrow x \equiv 0 \pmod{m}. \end{aligned}$$

(ii) is true.

$$\begin{aligned} x \equiv 0 \pmod{m} &\Rightarrow m | c \Rightarrow \text{there exists } y \text{ with } my = x \\ &\Rightarrow cmy = cx \Rightarrow cx \equiv 0 \pmod{cm}. \end{aligned}$$

(iii) is false. Take $c = m$, Then if $m \nmid x$ we do have $cx \equiv 0 \pmod{m}$ but $x \not\equiv 0 \pmod{m}$.
 (iv) is true.

$$x \equiv 0 \pmod{cm} \Rightarrow cm|x \Rightarrow \text{there exists } y \text{ with } x = cmy \Rightarrow x \equiv 0 \pmod{m}.$$

6. Determine the prime factorization of 192 and find the smallest POSITIVE exponent e such that $x^e \equiv 1 \pmod{192}$ for every value of x which is coprime to 192.

Solution. $192 = 2^6 \cdot 3$. We have $\phi(2^6) = 2^6 - 2^5 = 2^5 = 32$ and $\phi(3) = 2$. Hence we have

$$\begin{cases} x^{32} \equiv 1 \pmod{64} & \text{if } (x, 2) = 1 \\ x^{32} \equiv 1 \pmod{3} & \text{if } (x, 3) = 1 \end{cases} \Rightarrow x^{32} \equiv 1 \pmod{192} \text{ if } (x, 192) = 1.$$

However, let's check whether this is optimal. We check whether 32 is optimal for the modulus $2^6 = 64$. Let's compute powers of 3.

$$\begin{aligned} 3^2 &\equiv 9, \\ 3^4 &\equiv 9^2 \equiv 81 \equiv 17 \\ 3^8 &\equiv 17^2 \equiv 289 \equiv 33 \\ 3^{16} &\equiv 33^2 \equiv 1089 \equiv 1. \end{aligned}$$

It seems that 16 may work. We would like to show that every odd x is a solution to $x^{16} - 1 \equiv 0 \pmod{64}$. This is a tall order since checking it seems to involve calculating $x^{16} \pmod{64}$ for 32 values of x . Using the theorem about polynomial congruences can reduce this to 16 calculations. However, we recall that every odd x satisfies $x^2 \equiv 1 \pmod{8}$. This is better than expected since $\phi(8) = 4$. By successively squaring each equation below, we get k_0, k_1, k_2, k_3 such that

$$x^2 = 8k_0 + 1 \Rightarrow x^4 = 16k_1 + 1 \Rightarrow x^8 = 32k_2 + 1 \Rightarrow x^{16} = 64k_3 + 1.$$

This show that 16 does indeed work!

7. Determine the number of solutions to the equation $x^{16} \equiv 1 \pmod{41}$, and the number of solutions to the equation $x^{16} \equiv -1 \pmod{41}$.

By corollaries to Lagrange's theorem, the number of solutions to $x^{16} \equiv 1 \pmod{41}$ is $(16, 40) = 8$. The number os solutions to $x^{16} \equiv -1 \pmod{41}$ is $(32, 40) - (16, 40) = 8 - 8 = 0$.

8. Show that there are infinitely many primes of the form $6k + 1$.

This is the subject of homework question #8 in section 4.4. Suppose we have finitely many primes p_1, p_2, \dots, p_r of the form $6k + 1$, set $x = 6p_1 \cdots p_r$ and set

$$N = x^2 + x + 1.$$

Suppose that q is a prime divisor of N . We claim that q has the form $6k + 1$. First note that q cannot be 2 or 3 since these numbers divide x and so cannot divide N . Now since $(x - 1)(x^2 + x + 1) = x^3 - 1$, we have $q|x^3 - 1$. This implies in particular that $q \nmid x$. As a corollary to Fermat's theorem we get $x^{(q-1,3)} \equiv 1 \pmod{q}$. Now $(q - 1, 3)$ is either 1 or 3. If $(q - 1, 3) = 1$ then $x \equiv 1 \pmod{q}$ and $N \equiv 3 \pmod{q}$. But $q|N$, so $3 \equiv 0 \pmod{q}$ and $q = 3$. This cannot happen so $(q - 1, 3) = 3$ and $3|q - 1$ and since q is odd, $2|q - 1$ so indeed, q has the form $6k + 1$. Since q cannot be in the list p_1, \dots, p_r we see that there are infinitely many primes of the form $6k + 1$.