Extra problems: focused towards the last two weeks

Sunday, December 4, 2016 4:33 PM

1. Prove that, if d is a positive divisor of 2^n, then $d = 2^m$ for some integer $0 \le m \le n$.

[Hint. If $d=1$, then $d=2^0$. If $d \ge 2$, then it can be written as a product of irreducibles. Let p be an irreducible factor of d. So p is a prime, and $p \mid 2^n = \underbrace{2 \times 2 \times \cdots \times 2}_{n \text{ times}}$. Therefore $p \mid 2 \Rightarrow p = 2$. So any irreducible factor of d is 2. Hence $d = 2^m$ for some $m \in \mathbb{Z}^+$. Since $d \mid 2^n$, we have $d \le 2^n$. Therefore $m \le n$.]

2. Let $a_0 = 2$, $a_1 = 6$, $a_{n+1} = 6a_n - 4a_{n-1}$.

   (a) By induction on n, prove that $a_n = (3+\sqrt{5})^n + (3-\sqrt{5})^n$.

   (b) Use part (a) to prove $\lfloor (3+\sqrt{5})^n \rfloor = a_n - 1$.

   (c) Prove that $\gcd(a_n, a_{n+1})$ is a power of 2 for any $n \in \mathbb{Z}^+$.

[Hint. For part (b), use $0 < 3-\sqrt{5} < 1$ to conclude

$$(3+\sqrt{5})^n < a_n < (3+\sqrt{5})^n + 1.$$

- For part (c), notice $a_{n+1} \equiv -4a_{n-1} \pmod{a_n}$.

Hence $\gcd(a_{n+1}, a_n) = \gcd(a_n, -4a_{n-1})$. And $\gcd(a_n, -4a_{n-1})$ divides $4\gcd(a_n, a_{n-1})$. So by induction hypothesis $\gcd(a_{n+1}, a_n)$ divides a power of 2.

Thus by problem 1, it is a power of 2.]

Extra problems

Sunday, December 4, 2016 9:50 PM

3. For $a,b,c \in \mathbb{Z}^+$, prove that

$$\left.\begin{array}{l} \gcd(a,b)=1 \\ c \mid a \end{array}\right\} \Rightarrow \gcd(c,b)=1.$$

[Solution "quick" version:

$$d=\gcd(c,b) \Rightarrow \left.\begin{array}{l} d \mid b \\ \left.\begin{array}{l} d \mid c \\ c \mid a \end{array}\right\} \Rightarrow d \mid a \end{array}\right\} \Rightarrow d \mid \gcd(a,b) \Rightarrow d \mid 1 \Rightarrow d=1.]$$

4. For $a,b,c \in \mathbb{Z}^+$, prove that

$$\gcd(a,b)=1 \Rightarrow \gcd(a,bc)=\gcd(a,c).$$

[Solution 1 "quick" version:

$d_1=\gcd(a,bc)$ and $d_2=\gcd(a,c)$.

$$\left.\begin{array}{l} d_2 \mid a \\ d_2 \mid c \Rightarrow d_2 \mid bc \end{array}\right\} \Rightarrow d_2 \mid \gcd(a,bc) \Rightarrow d_2 \mid d_1.$$

$$\left.\begin{array}{l} d_1 \mid a \\ \gcd(a,b)=1 \end{array}\right\} \Rightarrow \left.\begin{array}{l} \gcd(d_1,b)=1 \\ d_1 \mid bc \end{array}\right\} \Rightarrow \left.\begin{array}{l} d_1 \mid c \\ d_1 \mid a \end{array}\right\} \Rightarrow d_1 \mid d_2.$$

Solution 2 "quick" version

$\exists x,y \in \mathbb{Z}$, $ax+by=1 \Rightarrow acx+bcy=c$.

$$\begin{aligned} \exists r,s \in \mathbb{Z},\ \gcd(a,c) &= ar+cs \\ &= ar+(acx+bcy)s \\ &= \text{integer linear combin. of } a \text{ and } bc \end{aligned}$$

$\Rightarrow \gcd(a,bc) \mid \gcd(a,c)$.

$\gcd(a,bc)$ is an int. line. comb. of a and $c \Rightarrow$ $\gcd(a,c) \mid \gcd(a,bc)$.]

Extra problems

Sunday, December 4, 2016 4:54 PM

5. Let $F_0, F_1, \ldots$ be the Fibonacci sequence. Show that

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

[Solution 1. Use $F_{n+1} \equiv F_{n-1} \pmod{F_n}$, induction

and $\left(a \overset{k}{\equiv} b \Rightarrow \gcd(a,k) = \gcd(b,k). \right)$

Solution 2. Use $F_n^2 - F_{n+1} \cdot F_{n-1} = (-1)^{n+1}$.]

6. Recall that long ago we used induction and

$$F_{n+m} = F_{m+1} F_n + F_m F_{n-1}$$

to prove that $k \mid n \Rightarrow F_k \mid F_n$. (Here again $F_0, F_1, \cdots$ is the Fibonacci sequence. In this exercise you will prove $\gcd(F_n, F_m) = F_{\gcd(n,m)}$.

(a) Suppose q and r are the quotient and the remainder of n divided by m. Prove that

$$F_n \equiv F_r \cdot F_{mq+1} \pmod{F_m}.$$

And conclude $\gcd(F_n, F_m) = \gcd(F_m, F_r)$.

(b) Use Euclid's algorithm and part (a) to show

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

Extra problems

Sunday, December 4, 2016 5:03 PM

[Solution: "quick" version

(a) $n = mq + r \Rightarrow$

$$F_n = F_{mq+r} = F_{mq+1} F_r + F_{mq} F_{r-1}$$

$$\Rightarrow F_n \equiv F_{mq+1} F_r \pmod{F_m} \text{ as } F_m \mid F_{mq}.$$

$$\Rightarrow \gcd(F_n, F_m) = \gcd(F_m, F_{mq+1} F_r).$$

$$\left.\begin{array}{l} \gcd(F_{mq}, F_{mq+1}) = 1 \\ F_m \mid F_{mq} \end{array}\right\} \Rightarrow \gcd(F_m, F_{mq+1}) = 1$$

$\Rightarrow$

$$\gcd(F_n, F_m) = \gcd(F_m, F_r).$$

(b) Suppose $n \geq m$, and let $a_0, a_1, \cdots, a_{n_0} = \gcd(m,n), a_{n_0+1} = 0$ be the sequence given by the Euclid's algorithm:

$a_0 = n$; $a_1 = m$; a_{k+1} is the remainder of a_{k-1} divided by a_k. By part (a), for any k, we have

$$\gcd(F_{a_{k-1}}, F_{a_k}) = \gcd(F_{a_k}, F_{a_{k+1}}).$$

Hence $\gcd(F_n, F_m) = \gcd(F_{a_{n_0}}, \underbrace{F_{a_{n_0+1}}}_{0}) = F_{a_{n_0}} = F_{\gcd(n,m)}$.]

Extra problems

Sunday, December 4, 2016 10:21 PM

7. Suppose $a, n \in \mathbb{Z}^+$. Let $L_{a,n} : \{0,1,\dots,n-1\} \to \{0,1,\dots,n-1\}$ be a function such that, for any $x \in \{0,1,\dots,n-1\}$, $L_{a,n}(x) \equiv ax \pmod{n}$. Prove that $L_{a,n}$ is a bijection if and only if $\gcd(a,n) = 1$.

[Solution "quick" version: ($\Rightarrow$)

$L_{a,n}$ is surjective $\Rightarrow \exists x,\ L_{a,n}(x) = 1$

$\Rightarrow \exists x,\ ax \overset{n}{\equiv} 1 \Rightarrow \gcd(a,n) = 1$.

($\Leftarrow$) $\gcd(a,n) = 1 \Rightarrow \exists a'$ s.t. $a'a \overset{n}{\equiv} 1$.

Consider $L_{a',n} \circ L_{a,n}$ and $L_{a,n} \circ L_{a',n}$.

$$\left(L_{a',n} \circ L_{a,n}\right)(x) \overset{n}{\equiv} a' L_{a,n}(x) \overset{n}{\equiv} a'ax \overset{n}{\equiv} x.$$

$\Rightarrow \left(L_{a',n} \circ L_{a,n}\right)(x) = x$ as $x, \left(L_{a',n} \circ L_{a,n}\right)(x)$ are in $\{0,1,\dots,n-1\}$.

Similarly $L_{a,n} \circ L_{a',n} = I$. Hence $L_{a,n}$ is invertible and so a bijection.]

8. Suppose $a, n \in \mathbb{Z}^+$, $b, c \in \mathbb{Z}$. Prove that

$$\left.\begin{array}{l} \gcd(a,n) = 1 \\ ab \overset{n}{\equiv} ac \end{array}\right\} \Rightarrow b \overset{n}{\equiv} c.$$

Extra problems

Sunday, December 4, 2016 10:33 PM

[<u>Solution</u> "quick" <u>version 1</u>. Use problem 7: $L_{a,n}$ is a bijection $\Rightarrow$ b and c divided by n have the same remainder $\Rightarrow$ $b \overset{n}{\equiv} c$.

<u>Solution</u> "quick" <u>version 2.</u>

$$\left.\begin{array}{l} n \mid a(b-c) \\ \gcd(n,a)=1 \end{array}\right\} \Rightarrow n \mid b-c \Rightarrow b \overset{n}{\equiv} c. \;]$$

9. Let p be an irreducible integer, and $a \in \mathbb{Z}$. Prove that

$$a^p \equiv a \pmod{p}$$

[<u>Solution</u> "quick" version. • $p \mid a \Rightarrow a^p \overset{p}{\equiv} 0 \overset{p}{\equiv} a$.

• $p \nmid a \Rightarrow \gcd(a,p)=1$ as p is irreducible.

$\Rightarrow L_{a,p}$ is a bijection.

Since $L_{a,p}(0)=0$, we have

$\{L_{a,p}(1), \ldots, L_{a,p}(p-1)\} = \{1, \ldots, p-1\}$. So

$$1 \cdot 2 \cdot \cdots \cdot (p-1) = L_{a,p}(1) \cdot \cdots \cdot L_{a,p}(p-1) \overset{p}{\equiv} (a)(2a) \cdots ((p-1)a)$$
$$= a^{p-1} \cdot 1 \cdot 2 \cdot \cdots \cdot (p-1).$$

$$\left.\begin{array}{l} p \text{ is irreducible} \Rightarrow p \text{ is prime} \\ p \nmid 1, p \nmid 2, \ldots, p \nmid p-1 \end{array}\right\} \Rightarrow p \nmid (p-1)!$$

$$\left.\begin{array}{l} \Rightarrow \gcd(p,(p-1)!)=1. \\ (p-1)! \overset{p}{\equiv} a^{p-1}(p-1)! \end{array}\right\} \Rightarrow a^{p-1} \overset{p}{\equiv} 1 \Rightarrow a^p \overset{p}{\equiv} a. \;]$$

Extra problems

Sunday, December 4, 2016 11:00 PM

10 ⓐ Find the remainder of 3^{1000} divided by 10.

[Solution "quick" version:

$3^2 \overset{10}{\equiv} -1 \Rightarrow (3^2)^{500} \overset{10}{\equiv} (-1)^{500}$

$\Rightarrow 3^{1000} \overset{10}{\equiv} 1$

$\Rightarrow$ 1 is the remainder.]

ⓑ Find the remainder of 2^{2017} divided by 13.

[Solution "quick" version: let's look at powers of 2 modulo 13. We use numbers $-6, -5, \dots, 6$.

$$\overset{0}{1}, \overset{1}{2}, \overset{2}{4}, \overset{3}{-5}, \overset{4}{3}, \overset{5}{6}, \overset{6}{-1}, \overset{7}{-2}, \overset{8}{-4}, \overset{9}{5}, \overset{10}{-3}, \overset{11}{-6}, \overset{12}{1}.$$

(Each time we multiply the previous number by 2 and find out what it is modulo 13). We find out that $2^{12} \equiv 1 \pmod{13}$.

$2017 = 12 \times 168 + 1$ $\Rightarrow$

$2^{2017} = (2^{12})^{168} \times 2 \overset{13}{\equiv} 2. \Rightarrow$ remainder is 2.]

Extra problem

Sunday, December 4, 2016 11:17 PM

11. Prove that for any $n \in \mathbb{Z}^+$ there is a multiple of n whose digits are either 0 or 1.

[Solution "quick" version: In class we showed for any $n+1$ integers $k_1, \dots, k_{n+1}$, there are $i \neq j$ such that $n \mid k_i - k_j$. Let

$k_1 = 1,\ k_2 = 11,\ \dots,\ k_{n+1} = \underbrace{11\cdots1}_{n+1 \text{ times}}$.

So $\exists\ 1 \le i < j \le n+1,\ n \mid \underbrace{1\cdots1}_{j} - \underbrace{1\cdots1}_{i} = \underbrace{11\cdots1}_{j-i}\underbrace{0\cdots0}_{i}$]

12. Prove that there is no perfect square of the form $13k+2$ for some integer k.

[Solution "quick" version $\forall a \in \mathbb{Z}$, a is congruent to $0, 1, \dots,$ or 12 modulo 13. $\Rightarrow$

$a \overset{13}{\equiv} 0, \pm1, \pm2, \pm3, \pm4, \pm5, \pm6 \Rightarrow$

$a^2 \overset{13}{\equiv} 0, 1, 4, 9, 3, 12, 10$. So

$a^2 \overset{13}{\not\equiv} 2$. (Similarly $a^2 \overset{13}{\not\equiv} 5, 6, 7, 8, 11$.).]

Extra problem

Sunday, December 4, 2016 11:36 PM

13. Find all the solutions of $2016\, x \overset{109}{\equiv} 2017$.

[Solution. $2016 = 109 \times 18 + 54$

and $2017 = 109 \times 18 + 55$

So we have to solve $54\, x \overset{109}{\equiv} 55$

$\Rightarrow \quad 2 \times 54\, x \overset{109}{\equiv} 2 \times 55$

$\Rightarrow \quad -x \overset{109}{\equiv} 1 \Rightarrow x \overset{109}{\equiv} -1$.

Let's check if the converse hold:

$-2016 \equiv 2017 \pmod{109} \Leftarrow 2017 + 2016 \overset{109}{\equiv}$

$55 + 54 \overset{109}{\equiv} 0$.]

14. Find all the solutions of $9x \equiv 8 \pmod{23}$

[Solution 1 Ad hoc method.

$9x \overset{23}{\equiv} 8 \Rightarrow 3 \times 9x \overset{23}{\equiv} 3 \times 8$

(multiply by numbers to get simpler coeff.)

$\Rightarrow 4x \overset{23}{\equiv} 1$

$\Rightarrow 6 \times 4x \overset{23}{\equiv} 6$

$\Rightarrow x \overset{23}{\equiv} 6$

Check the converse: $9 \times 6 \equiv 54 \overset{23}{\equiv} 8$. ✓.

Extra problems

Sunday, December 4, 2016 11:53 PM

Solution 2. Use Euclid's algorithm to find a modular inverse of 9 modulo 23:

$$23 = 9\times 2 + 5$$
$$9 = 5\times 1 + 4$$
$$5 = 4\times 1 + 1 \rightarrow 1 = 5 - 4\times 1$$
$$4 = 1\times 4 + 0$$

$$= 5 - (9 - 5\times 1)\times 1$$
$$= 9\times(-1) + 5\times 2$$
$$= 9\times(-1) + (23 - 9\times 2)\times 2$$
$$= 23\times 2 + 9\times(-5)$$

$\Rightarrow$ -5 is a modular inverse of 9 modulo 23.

$$\Rightarrow (-5)(9x) \overset{23}{\equiv} (-5)(8)$$

$$\Rightarrow x \overset{23}{\equiv} -40 \equiv 46-40 \equiv 6.$$

Now one can check the converse.]