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

   [Hint: If \( d = 1 \), then \( d = 2^0 \). If \( d \geq 2 \), then it can be written as a product of irreducibles. Let \( p \) be an irreducible factor of \( d \). So \( p \) is a prime, and \( p \mid 2^n = 2 \times 2 \times \cdots \times 2 \) \( n \) 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 \( d \leq 2^n \). Therefore \( m \leq n \).]

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

$$\text{gcd}(a,b) = 1 \Rightarrow \text{gcd}(c,b) = 1$$

$$c \mid a$$

[Solution "quick" version:

$$d = \text{gcd}(c,b) \Rightarrow d \mid b \quad \Rightarrow d \mid \text{gcd}(a,b)$$

$$d \mid c \Rightarrow d \mid a \quad \Rightarrow d \mid 1 \Rightarrow d = 1.$$]

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

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

[Solution 1 "quick" version:

$$d_1 = \text{gcd}(a,bc) \quad \text{and} \quad d_2 = \text{gcd}(a,c).$$

$$d_2 \mid a \Rightarrow d_2 \mid \text{gcd}(a,bc) \Rightarrow d_2 \mid d_1.$$  

$$d_2 \mid c \Rightarrow d_2 \mid bc.$$  

$$d_1 \mid a \Rightarrow \text{gcd}(d_1,b) = 1 \Rightarrow d_1 \mid c \Rightarrow d_1 \mid d_2.$$  

Solution 2 "quick" version

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

$$\exists r, s \in \mathbb{Z}, \ \text{gcd}(a,c) = ar + cs$$

$$= ar + (acx + bcy)s$$

$$= \text{integer linear comb. of a and bc}.$$  

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

$$\text{gcd}(a,bc) \text{ is an int. lin. comb. of a and c \Rightarrow}$$

$$\text{gcd}(a,c) \mid \text{gcd}(a,bc).$$]
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 \[ (a \equiv b \Rightarrow \gcd(a, k) = \gcd(b, k)). \]

**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 $k | n \Rightarrow F_k | F_n$. (Here again $F_0, F_1, \ldots$ is the Fibonacci sequence. In this exercise you will prove 
\[ \gcd (F_n, F_m) = F_{\gcd(n,m)}. \]

@ Suppose $q$ and $r$ are the quotient and the remainder of $n$ divided by $m$. Prove that 
\[ F_n \equiv F_r \cdot F_{m,q+1} \pmod{F_m}. \]

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

@ Use Euclid's algorithm and part @ to show 
\[ \gcd (F_n, F_m) = F_{\gcd(n,m)}. \]
Extra problems

Sunday, December 4, 2016 5:03 PM

Solution: \( n = mq + r \) \( \Rightarrow \)

\[
F_n = F_{mq+r} = F_{mq+1}F_r + F_mF_{r-1}
\]

\( \Rightarrow F_n = F_{mq+1}F_r \pmod{F_m} \) as \( F_m \mid F_{mq} \).

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

\[
gcd(F_{mq}, F_{mq+1}) = 1 \Rightarrow gcd(F_m, F_{mq+1}) = 1
\]

\( F_m \mid F_{mq} \)

\[
gcd(F_n, F_m) = gcd(F_m, F_r).
\]

(6) Suppose \( n \geq m \), and let \( a_0, a_1, \ldots, a_n = gcd(m, m), a_{n+1} = 0 \)
be the sequence given by the Euclid’s algorithm:

\[
a_0 = n; \ a_1 = m; \ a_{k+1} \text{ is the remainder of } a_k \div a_{k-1}
\]

By part (6), for any \( k \), we have

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

Hence

\[
gcd(F_n, F_m) = gcd(F_{a_0}, F_{a_{n+1}}) = F_{a_0}F_{gcd(m, m)}.
\]
7. Suppose \(a, n \in \mathbb{Z}^+\). Let \(L_{a, n} : \{0, 1, \ldots, n-1\} \rightarrow \{0, 1, \ldots, n-1\}\) be a function such that, for any \(x \in \{0, 1, \ldots, n-1\}\),
\[L_{a, n}(x) \equiv ax \pmod{n}.
\]Prove that \(L_{a, n}\) is a bijection if and only if \(\gcd(a, n) = 1\).

\[\text{Solution “quick” version: } (\Leftrightarrow)\]

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

\(\Rightarrow \exists x, \ ax \equiv 1 \Rightarrow \gcd(a, n) = 1\).

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

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

\[(L_{a', n} \circ L_{a, n})(x) \equiv a'L_{a, n}(x) \equiv a'a \equiv 1 \times x \equiv x.\]

\(\Rightarrow \ (L_{a', n} \circ L_{a, n})(x) = x \text{ as } x, (L_{a', n} \circ L_{a, n})(x) \text{ are in } \{0, 1, \ldots, 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
\[
\gcd(a, n) = 1 \quad \Rightarrow \quad b \equiv c \pmod{n}
\]
\[ab \equiv ac \]

Extra problems
Sunday, December 4, 2016   10:33 PM

Solution “quick” version 1. Use problem 7: \( L_{a,n} \) is a bijection \( \Rightarrow \) \( b \) and \( c \) divided by \( n \) have the same remainder \( \Rightarrow b \equiv c \).

Solution “quick” version 2.

\[
\begin{align*}
n \mid a(b-c) \Leftrightarrow n \mid b-c \Rightarrow b \equiv c. \\
gcd(n,a)=1 \quad \Box
\end{align*}
\]

9. Let \( p \) be an irreducible integer, and \( a \in \mathbb{Z} \). Prove that \( a^p \equiv a \pmod{p} \).

Solution “quick” version. • \( p \mid a \Rightarrow a^p \equiv 0 \equiv a \).
• \( p \nmid a \Rightarrow gcd(a,p)=1 \) as \( p \) is irreducible.

\[ \Rightarrow L_{a,p} \text{ is a bijection.} \]

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

\[
\begin{align*}
\{ L_{a,p}(1), \ldots, L_{a,p}(p-1) \} &= \{ 1, \ldots, p-1 \} \quad \because \quad 1 \cdot 2 \cdot \cdots \cdot (p-1) = L_{a,1}(1) \cdots L_{a,p}(p-1) \\
&= a^p \cdot 1 \cdot 2 \cdot \cdots \cdot (p-1) \\
p \text{ is irreducible } \Rightarrow p \text{ is prime } \Rightarrow p \nmid (p-1)! \\
p \nmid 1, p \nmid 2, \ldots, p \nmid p-1 \Rightarrow gcd(p, (p-1)!) = 1 \Rightarrow a^{p-1} \equiv 1 \Rightarrow a^p \equiv a. 
\end{align*}
\]
10. Find the remainder of $3^{1000}$ divided by 10.

Solution "quick" version:

$$3^2 \equiv -1 \Rightarrow (3^2)^{500} \equiv 10 \equiv (-1)^{500} \Rightarrow 3^{1000} \equiv 1$$

$\Rightarrow 1$ is the remainder.

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

Solution "quick" version: let’s look at powers of 2 modulo 13. We use numbers $-6,-5,-4,-3,-2,-1,0,1,2,3,4,5,6,7,8,9,10,11,12$. (Each time we multiply the previous number by 2 and find out what it is modulo 13). We find out that $2^{12} \equiv 1 \pmod{13}$. $\Rightarrow$

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

$$2^{2017} = (2^{12})^{168} \times 2 \equiv 2 \pmod{13} \Rightarrow \text{remainder is 2.}$$
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 \( k_1, \ldots, k_{n+1} \), there are \( i \neq j \) such that \( n \mid k_i - k_j \). Let \( k_1 = 1, k_2 = 11, \ldots, k_{n+1} = \underbrace{11 \ldots 1}_{n+1 \text{ times}} \).

So \( \exists 1 \leq i < j \leq n+1, n \mid \underbrace{1 \ldots 1 - 1 \ldots 1}_{j-i} = \underbrace{10 \ldots 0}_i \) \( \text{mod } j \).

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, \ldots, or 12 modulo 13. \( \Rightarrow \)

\( a^{\frac{13}{2}} \equiv 0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6 \Rightarrow \)

\( a^{\frac{13}{2}} \equiv 0, 1, 4, 9, 3, 12, 10 \). So

\( a^{\frac{13}{2}} \neq 2 \). (Similarly \( a^{\frac{13}{2}} \neq 5, 6, 7, 8, 11 \).) \]
13. Find all the solutions of \( 2016 \equiv 2017 \). 

**Solution.** \( 2016 = 109 \times 18 + 54 \) and \( 2017 = 109 \times 18 + 55 \). So we have to solve \( 54 \equiv 109 \). 

\[ 2 \times 54 \equiv 2 \times 55 \]

\[ \Rightarrow -x \equiv 1 \Rightarrow x \equiv -1. \]

Let’s check if the converse holds:

\[ -2016 \equiv 2017 \pmod{109} \iff 2017 + 2016 \equiv 55 + 54 \equiv 0. \]

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

**Solution 1** Ad hoc method.

\[ 9x \equiv 8 \Rightarrow 3 \times 9x \equiv 3 \times 8 \]

Multiply by numbers to get simpler coeff.: \( 4x \equiv 1 \)

\[ \Rightarrow 6 \times 4x \equiv 6 \]

\[ \Rightarrow x \equiv 6 \]

Check the converse: \( 9 \times 6 \equiv 54 \equiv 8 \).
Solution 2. Use Euclid's algorithm to find a modular inverse of 9 modulo 23:

\[ 23 = 9 \times 2 + 5 \]
\[ 9 = 5 \times 1 + 4 \]
\[ 5 = 4 \times 1 + 1 \rightarrow 1 = 5 - 4 \times 1 \]
\[ 4 = 1 \times 4 + 0 \rightarrow 5 = 5 - (9 - 5 \times 1) \times 1 \]
\[ = 9 \times (-1) + 5 \times 2 \]
\[ = 9 \times (-1) + (23 - 9 \times 2) \times 2 \]
\[ = 23 \times 2 + 9 \times (-5) \]

\[ \Rightarrow -5 \text{ is a modular inverse of } 9 \text{ modulo } 23. \]

\[ \Rightarrow (-5)(9x)^{23} \equiv (-5)(8) \]
\[ \Rightarrow x^{23} \equiv -40 \equiv 46 - 40 \equiv 6. \]

Now one can check the converse. \( \Box \)