Solutions to Assignment 2

4. a)

$$\begin{aligned} 30030 &= 116 \cdot 257 + 218 \\ 257 &= 218 + 39 \\ 218 &= 5 \cdot 39 + 23 \\ 39 &= 23 + 16 \\ 23 &= 16 + 7 \\ 16 &= 2 \cdot 7 + 2. \\ 7 &= 3 \cdot 2 + 1 \end{aligned}$$

$\gcd(30030, 257) = 1.$

b) $\sqrt{257} \cong 16$ and the primes less than 16 are 2, 3, 5, 7, 11 and 13. $30030 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$. If 257 was not prime then the gcd with one of these primes would not be 1. But then the $\gcd(30030, 257)$ would not be 1 which it is so 257 is prime.

6. a) After F_2, the Fibonacci sequence is increasing. So the result of dividing F_{n+1} by F_n is F_{n-1} since $F_{n+1} = F_n + F_{n-1}$ and $F_{n-1} < F_n$. This says that the Euclidean algorithm applied to F_n and F_{n-1} looks like

$$\begin{aligned} F_n &= F_{n-1} + F_{n-2} \\ F_{n-1} &= F_{n-2} + F_{n-3} \\ &\vdots \\ 3 &= 2 + 1 \end{aligned}$$

so $\gcd(F_n, F_{n-1}) = 1$

b) $\gcd(1111111, 11111) = 1$ as

$$\begin{aligned} 1111111 &= 10^3 \cdot 11111 + 111 \\ 11111 &= 10^2 \cdot 111 + 11 \\ 111 &= 10 \cdot 11 + 1 \end{aligned}$$

c) To say that b is F_n many 1's repeated means

$$b = 1 + 10 + 100 + \cdots + 10^{F_{n-1}} = \sum_{k=1}^{F_n - 1} 10^k$$

and likewise $a = \sum_{k=1}^{F_{n-1}-1} 10^k$

One step of the Euclidean algorithm for gcd (b,a) gives:

$$b = \sum_{k=1}^{F_n - 1} 10^k = \underset{\substack{\uparrow \\ \text{Shift right} \\ F_{n-2} \text{ places.}}}{10^{F_{n-2}}} \sum_{k=1}^{F_{n-1}-1} 10^k + \sum_{k=1}^{F_{n-2}-1} 10^k$$

and so on as, we repeat this inductively and get gcd (b, a) = 1.

14. a) $7^7 \equiv (-1)^7 \bmod 4$
$\equiv -1 \bmod 4.$

b) By Fermat, $7^{7^7} \equiv 7^3 \bmod \cancel{5}$ since $7^7 \equiv 3 \bmod 4.$
$\equiv 2^3 \bmod 5$
$\equiv 3 \bmod 5$

and $7^{7^7} \equiv 1 \bmod 2$ so by the Chinese Remainder Theorem, $7^{7^7} \equiv 3 \bmod 10$, That is, its last digit is 3.

15 a) These results rely on you looking very closely at the value of $\phi(1)$:

$\phi(1) = \#$ of a, $1 \le a \le 1$, s.t. $\gcd(a, 1) = 1$

That is, $\phi(1) = 1$.

So $\phi(1) = 1$, $\phi(2) = 1$, $\phi(5) = 4$, $\phi(10) = 4$.

$10 = 1 + 1 + 4 + 4$.

b) $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(6) = 2$
$\phi(12) = 4$.

$12 = 1 + 1 + 2 + 2 + 2 + 4$.

c) Conjecture : $\phi(n) = \sum_{d|n} \phi(d)$.

18. a) $\left| \begin{pmatrix} 1 & 1 \\ 6 & 1 \end{pmatrix} \right| = -5$ and -5 is invertible mod 26.

$(5 \cdot (-5) \equiv 1 \mod 26)$.

So this matrix is invertible. It's inverse is

$$5 \begin{pmatrix} 1 & -1 \\ -6 & 1 \end{pmatrix} \text{ mod } 26 \quad \text{or} \quad \begin{pmatrix} 5 & 21 \\ 22 & 5 \end{pmatrix}$$

b) $\begin{vmatrix} 1 & 1 \\ b & 1 \end{vmatrix} = 1 - b$ and $1-b$ is invertible mod 26

as long as $1-b$ is not even or 13. So $b \equiv$ any even number except -12 mod 26.

20. a) Since the $\gcd(a,n) = 1$, by Euler's theorem
$a^{\phi(n)} \equiv 1 \bmod n$ so $\operatorname{ord}_n(a) \leq \phi(n)$.

b) If $r = \operatorname{ord}_n(a)$ then $a^r \equiv 1 \bmod n$ so
$(a^r)^k \equiv 1 \bmod n$ i.e. $a^m = a^{rk} \equiv 1 \bmod n$.

c) If $t = qr + s$ and $a^t \equiv 1 \bmod n$ then
$1 \equiv a^{qr+s} \equiv a^{qr} \cdot a^s \equiv a^s \bmod n$.

d) So if s is as in part c), then $a^s \equiv 1 \bmod n$ and since r is the least positive integer to do this, s must be 0. So if $a^t \equiv 1 \bmod n$ for $t > 0$ then $r \mid t$.

e) From a) and d) then $\operatorname{ord}_a(n) \mid \phi(n)$.