MAT315 Homework - 4 Rui Qiu #999292809

1. (14.2).

$F_k = 2^{2^k} + 1$

$F_1 = 5$

$F_2 = 17$

$F_3 = 257$

$F_4 = 65537$ #

...

Fermat primes.

Need to show $\gcd(F_k, F_m) = 1$ for $k \neq m$.

Solution: Suppose $k > m$.

$F_k = 2^{2^k} + 1$

$F_k - 2 = 2^{2^k} + 1 - 2 = 2^{2^k} - 1 = (2^{2^{k-1}} + 1)(2^{2^{k-1}} - 1)$

$= (2^{2^{k-1}} + 1)(2^{2^{k-2}} + 1)(2^{2^{k-2}} - 1)$

$= \cdots$

$= (2^{2^{k-1}} + 1) \cdots (2^{2^0} + 1)(2^{2^0} - 1)$

$= \prod_{i=0}^{k-1} (2^{2^i} + 1)$

Since $m < k$, then $(2^{2^m} + 1)$ must be in the product of $2^{2^i} + 1$ from $i = 0$ to $i = k-1$.

Therefore $2^{2^m} + 1 \mid F_k - 2$

i.e. $F_m \mid F_k - 2$

both F_m and F_k are odd.

Therefore, $\gcd(F_k, F_m) = 1$ for $k \neq m$.

2. (15.1)

$\sigma(n)$ = sum of all divisors of n (including 1 & n).

to show $\gcd(m,n)=1$, $\sigma(mn)=\sigma(m)\sigma(n)$

Proof: Suppose $m = p_1 p_2 \cdots p_r$

$n = q_1 q_2 \cdots q_s$

and $\gcd(p_i, q_j)=1$ for all $i \in [1, r]$, $j \in [1, s]$.

$$\sigma(m) = 1 + p_1 + p_2 + \cdots + p_r + p_1p_2 + \cdots + p_1p_2\cdots p_r = \sum_{d|m} d$$

$$\sigma(n) = 1 + q_1 + \cdots + q_s + q_1q_2 + \cdots + q_1q_2\cdots q_s = \sum_{d|n} d$$

We rename the divisors of m to be $a_1, a_2, \cdots, a_k$.

the divisors of n to be $b_1, b_2, \cdots, b_l$.

Claim: Divisors of mn are $a_i b_j$, $i=1,\cdots,k$, $j=1,\cdots,l$.

Suppose $t \mid mn$, either $t \mid m$ or $t \mid n$ or both

~~(the only case that $t|m$ and $t|n$ is $t=1$ since $\gcd(m,n)=1$)~~

so

① $t \mid m \Rightarrow t = a_i$, $t = a_i b_1 = a \cdot 1$

② $t \mid n \Rightarrow t = b_j$, $t = a_1 b_j = 1 \cdot b_j$

③ $t \mid mn \Rightarrow t = a_i b_j$

Therefore divisors of mn are all of the form $a_i b_j$.

So for $\sigma(m)$ many divisors $a_i \mid m$,

$\sigma(n)$ many divisors $b_j \mid n$.

~~Then~~ Their products:

$\sigma(m)\sigma(n)$ many divisors $a_i b_j \mid mn$

Hence $\sigma(mn) = \sigma(m)\sigma(n)$.

■

3. (15.3(b,e))

(b). If p is odd prime, p^k can never be a perfect number.

Proof: sum of proper divisors of p^k is

$$p^0+p^1+\cdots+p^{k-1} = 1+\cdots+p^{k-1} = \frac{p^k-1}{p-1}$$

Claim p^k is a perfect number:

$$p^k = \frac{p^k-1}{p-1}$$

~~$p^{k+1} - p^k = p^k$~~ ~~$= 1$~~ since p is odd prime

~~$p^k(p-1) = p^k$~~ ~~$= 1$~~ so $p \geq 2$, $p-1 \geq 1$

~~$p^{k+1} - 2p^k + 1 = 0$~~ so $p^k(p-1) \geq p^k > p^k - 1$

Hence p^k is not a perfect number.

~~$\neq p^k$~~

Therefore p^k can never be a perfect number.

(e). If p, q are distinct odd primes, then a number of the form $q^i p^j$ can never be a ~~distin~~ perfect number.

Proof: Since p, q are distinct odd primes, $\gcd(p,q) = 1$.

$$\sigma(q^i p^j) = \sigma(q^i)\sigma(p^j)$$

$$= \frac{q^{i+1}-1}{q-1}\,\frac{p^{j+1}-1}{p-1}$$

$$= \frac{(p^{j+1}-1)(q^{i+1}-1)}{(p-1)(q-1)}$$

$\sigma(q^i p^j)$ is the number of all divisors of $q^i p^j$

so number of proper divisors of $q^i p^j$ is $\sigma(q^i p^j) - q^i p^j$

Suppose $q^i p^j$ is perfect, then.

$$\frac{(p^{j+1}-1)(q^{i+1}-1)}{(p-1)(q-1)} = 2p^j q^i$$

So $2p^j q^i (p-1)(q-1) = (p^{j+1}-1)(q^{i+1}-1)$

$2p^j q^i (pq - p - q + 1) = p^{j+1}q^{i+1} - q^{i+1} - p^{j+1} + 1$

$2p^{j+1}q^{i+1} - 2p^{j+1}q^i - 2p^j q^{i+1} + 2p^j q^i = p^{j+1}q^{i+1} - q^{i+1} - p^{j+1} + 1$

$p^j q^i (pq - 2p - 2q + 2) = 1 - q^{i+1} - p^{j+1}$

RHS < 0

LHS:

claim $pq > 2(p+q-1)$

$\frac{1}{2}pq + \frac{1}{2}pq > 2p + 2q - 2$

Since p, q are distinct odd prime.

so $p=3, q=5$ the base case:

$15 > 2(3+5-1) = 14$ ✓

For $p, q \geq 5$.

$\frac{1}{2}pq > 2p$

$\frac{1}{2}pq > 2q$

So $\frac{1}{2}pq + \frac{1}{2}pq > 2p + 2q > 2p + 2q - 2$.

So LHS > 0.

So have a contradiction.

Therefore $q^i p^j$ can never be a perfect number. ∎

4. (15.6(b2))

m	product of factors
6	$1\times2\times3=6$
15	$1\times3\times5=15$
21	$1\times3\times7=21$
26	$1\times2\times13=26$
33	$1\times3\times11=33$
34	$1\times2\times17=34$
35	$1\times5\times7=35$
⋮	

If a number m can be written as the form $m=pq$ where p,q are two distinct primes. then m is product perfect.

5. (16.3(a))

Solution: (Successive squaring)

① $7386 = 2^1+2^3+2^4+2^6+2^7+2^{10}+2^{11}+2^{12}$

② $7^1 \equiv A_0 \bmod 7387$

$7^2 \equiv 49 = A_1 \bmod 7387$

$7^4 \equiv 2401 = A_2 \bmod 7387$

$7^8 \equiv 5764801 \equiv 2941 \bmod 7387 \equiv A_3 \bmod 7387$

$7^{16} \equiv 6691 \bmod 7387 \equiv A_4 \bmod 7387$

$7^{32} \equiv 4261 \bmod 7387 \equiv A_5 \bmod 7387$

$7^{64} \equiv 6262 \bmod 7387 \quad (A_6)$

$7^{128} \equiv 2448 \bmod 7387 \quad (A_7)$

$7^{256} \equiv 1847 \bmod 7387 \quad (A_8)$

$7^{512} \equiv 6002 \bmod 7387 \quad (A_9)$

$7^{1024} \equiv 4492 \bmod 7387 \quad (A_{10})$

$7^{2048} \equiv 3713 \bmod 7387 \quad (A_{11})$

$7^{4096} \equiv 2227 \bmod 7387 \quad (A_{12})$

③ Then $A_0^0 \cdot A_1^1 \cdots A_{12}^1 \bmod 7387$

$= 49\times2941\times6691\times6262\times2448\times4492\times3713\times2227 \bmod 7387$

$= 702 \bmod 7387$

$A_2 \equiv 452^4 \bmod 1147 \equiv 692$

$A_3 \equiv 565 \bmod 1147$

$A_4 \equiv 359 \bmod 1147$

$A_5 \equiv 417 \bmod 1147$

$A_6 \equiv 692 \bmod 1147$

$A_7 \equiv 565 \bmod 1147$

$A_8 \equiv 359 \bmod 1147$

$A_9 \equiv 417 \bmod 1147$

$$452^{929} \bmod 1147$$
$$\equiv 452 \times 417 \times 565 \times 359 \times 417 \bmod 1147$$
$$\equiv 763 \bmod 1147$$

So $x = 763$

Since $\gcd(7, 7387) = 1$, if 7387 is a prime then
$a^{m-1} \bmod m \equiv 1 \bmod m$ by Fermat's Little Thm.
But we know $a^{m-1} \bmod m \equiv 702$
In fact $7387 = 83 \times 89$.

6. (17.1)

$$x^{329} \equiv 452 \bmod 1147$$

Solution:

$1147 = 31 \times 37$

$\phi(1147) = \phi(31)\phi(37) = 30 \times 36 = 1080$

need to find u, v s.t.

$$329u - 1080v = 1$$

$1080 = 329 \times 3 + 93$

$329 = 93 \times 3 + 50$

$93 = 50 \times 1 + 43$

$50 = 43 \times 1 + 7$

$43 = 7 \times 6 + 1$

$1 = 43 - 7 \times 6$

$= (93 - 50) - (50 - 43) \times 6$

$= (1080 - 329 \times 3) - (329 - 93 \times 3)$

$- 6 \times (329 - 93 \times 3) + 6 \times (93 - 50)$ —

$= 1080 - 329 \times 3 - 329 + 3 \times (1080 - 329 \times 3)$

$- 6 \times 329 + 18 \times (1080 - 329 \times 3)$ ~~$- 329 + 3 \times (1080 - 329 \times 3)$~~

$= $ ~~$25 \times 1080 - 83 \times 329$~~ $+ 6 \times (1080 - 3 \times 329) - 6 \times (329 - 93 \times 3)$

$6 \times (329 - 3 \times (1080 - 329 \times 3))$

$929 \times 329 - 1080 \times 283 = 1$

so $u = 929$

$v = 283$

Compute $452^{929} \bmod 1147$ by successive squaring

$929 = 512 + 256 + 128 + 32 + 1$

(9 8 7 5 0)

$A_0 \equiv 452^1 \bmod 1147$

$A_1 \equiv 452^2 \bmod 1147 \equiv 138$