MAT 315 Solutions for Homework #4 – 6

Homework #4

1. We show $F_m \mid F_k - 2$ if $k > m$.

Then if $\gcd(F_k, F_m) = d$, $d \mid F_m$, $d \mid F_k$

So $d \mid F_k - 2 \Rightarrow d \mid 2$

Since F_k is odd, $d = 1$.

$$F_k - 2 = 2^{2^k} - 1 = \left(2^{2^{m+1}}\right)^{2^{k-m-1}} - 1$$

$$= \left(2^{2^{m+1}} - 1\right)\left(\left(2^{2^{m+1}}\right)^{2^{k-m-1}-1} + \cdots + 1\right)$$

Here $2^{2^{m+1}} - 1 = \left(2^{2^m}+1\right)\left(2^{2^m}-1\right)$.

2. Let $d_1, \ldots, d_r$ be divisors of m
$e_1, \ldots, e_s$ 〃 n.

Claim: $d_i e_j$, $i = 1, \ldots, r$, $j = 1, \ldots, s$ are divisors of mn.

Clearly, $d_i e_j \mid mn$.

Conversely, let d be a divisor of mn.

Let $d_i = \gcd(d, m)$, $e_j = \gcd(d, n)$.

Then $d = d_i e_j$ (omit the proof.)

Hence $\sigma(mn) = \sum_{i,j} d_i e_j = \left(\sum_i d_i\right)\left(\sum_j e_j\right)$

$= \sigma(m)\sigma(n)$

3. $\sigma(p^k) = 1 + p + \cdots + p^k = \frac{p^{k+1}-1}{p-1}$

If $\sigma(p^k) = 2p^k$, $p^{k+1} - 1 = 2p^k(p-1)$.

So p divides $p^{k+1} - 1$. Contradiction

or $\sigma(p^k) = \frac{p^{k+1}-1}{p-1} < \frac{p^{k+1}}{p-1} = \frac{p}{p-1} p^k < 2p^k$

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

$$< \frac{p}{p-1} p^j \cdot \frac{q}{q-1} q^i$$

Show that $\frac{p}{p-1} \cdot \frac{q}{q-1} \leq 2$.

[$2(p-1)(q-1) - pq = (p-2)(q-2) - 2 \geq 3$
if p, q distinct odd primes.]

4. If n is product perfect and has at least two prime factors p, q, then

$$n \geq \frac{n}{p} \cdot \frac{n}{q} = \frac{n^2}{pq}$$

So $n \leq pq \leq n \Rightarrow n = pq$.

If $n = p^k$ is product perfect,

$1 \cdot p \cdot p^2 \cdots p^{k-1} = p^k$

$\Rightarrow p^{1+2+\cdots+k-1} = p^{\frac{k(k-1)}{2}} = p^k$

So $k = 3$.

5. $7^{7386} \equiv 702 \pmod{7387}$

By Fermat's little theorem,
7387 is not a prime.

6. $1147 = 31 \times 37$

$\phi(1147) = 30 \times 36 = 1080$.

Next we solve $329u - 1080v = 1$.

$u = 929$, $v = 283$.

The solution is

$x = 452^{929} \equiv 763 \pmod{1147}$

Homework #5

1. $7081 = 73 \times 97$. $\phi(7081) = 72 \times 96 = 6912$.

Solve $1789u - 6912v = 1$.

$u = 85$.

Compute $5192^{85} \equiv 1615 \pmod{7081}$

$2604^{85} \equiv 2823 \pmod{7081}$

$4222^{85} \equiv 1130 \pmod{7081}$

So the message is "Fermat."

2. If $p \equiv 2 \pmod 3$, any a is a cubic residue.

If $a \equiv 0 \pmod p$, clear.

Suppose $a \not\equiv 0 \pmod p$. Then $a^{p-1} \equiv 1 \pmod p$.

Let $p = 3k+2$. $a^p \equiv a \pmod p$

$a = 1 \cdot a \equiv a^{3k+1} \cdot a^{3k+2} = a^{6k+3} = (a^{2k+1})^3 \bmod p$.

3. (1) $5987 \equiv 3 \pmod 4$.

no solution

(2) $x^2 - 64x + 943 = (x-32)^2 - 81 \equiv 0 \bmod 3011$

Since $81 = 9^2$, a solution exists.

In fact, $x - 32 \equiv \pm 9 \bmod 3011$.

4. If $p = 2$, $x^2 \equiv 3 \pmod 2$ has a sol. $x \equiv 1$

If $p = 3$, $x^2 \equiv 3 \pmod 3$ has a sol $x \equiv 0$.

Assume $p > 3$.

Then $x^2 \equiv 3 \pmod p$ has a sol

$\Leftrightarrow \left(\frac{3}{p}\right) = 1$.

If $p \equiv 1 \bmod 4$, $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = 1$.

$p \equiv 1 \bmod 3$.

In this case, $p \equiv 1 \bmod 12$.

If $p \equiv 3 \bmod 4$, $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = 1$.

So $p \equiv 2 \bmod 3$.

In this case, $p \equiv 11 \bmod 12$.

5. Since $p = 5k+2$, and p is odd, $k = 2l+1$.

So $p = 10l + 7$. $\frac{p-1}{2} = 5l + 3$.

We divide $5, 10, 15, \ldots, 5 \cdot \frac{p-1}{2}$ into

$5, 10, \ldots, 5l$;

$5(l+1), 5(l+2), \ldots, 5(2l+1)$;

$5(2l+2), 5(2l+3), \ldots, 5(3l+2)$;

$5(3l+3), 5(3l+4), \ldots, 5(4l+2)$;

$5(4l+3), 5(4l+4), \ldots, 5(5l+3)$.

Here, $5(l+1), \ldots, 5(2l+1)$ are reduced to

$-(5l+2), -(5l-$[redacted]$3), \ldots,$ [redacted] -2 ; $l+1$ negative values

$5(3l+3), \ldots, 5(4l+2)$ are reduced to

$-(5l-1), -(5l-6), \ldots, -4$; l negative values

Hence $5^{\frac{p-1}{2}} \equiv (-1)^{2l+1} = -1 \bmod p$.

6. Suppose $p_1 \ldots p_r$ are distinct primes $\equiv 1 \bmod 3$

Consider $A = (2p_1 \cdots p_r)^2 + 3 = q_1 \cdots q_s$ q_i odd primes.

Claim: (1) $q_i \neq p_j$ for each i, j

(2) $q_i \equiv 1 \bmod 3$

(1) is clear since $q_i \mid A$, but $p_j \nmid A$

For (2), $A \equiv 0 \mod q_i$

So $x^2+3 \equiv 0 \mod q_i$ has a sol.

So $\left(\frac{-3}{q_i}\right)=1$.

By quadratic reciprocity,

$$1=\left(\frac{-3}{q_i}\right)=\left(\frac{-1}{q_i}\right)\left(\frac{3}{q_i}\right)=\left(\frac{-1}{q_i}\right)\left(\frac{q_i}{3}\right)(-1)^{\frac{q_i-1}{2}}$$

$$=\left(\frac{q_i}{3}\right) \Rightarrow q_i \equiv 1 \mod 3.$$

Homework #6.

1. Since $p \equiv 3 \mod 4$, $\frac{p+1}{4}$ is an integer.

$x=a^{\frac{p+1}{4}} \Rightarrow x^2=a^{\frac{p+1}{2}}=a^{\frac{p-1}{2}}\cdot a \equiv a \mod p$

since by Euler's criterion,

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)=1 \mod p.$$

$7^{197} \equiv 105 \pmod{187}$.

2. Since $p \equiv 5 \pmod 8$, $\frac{p+3}{8}$ and $\frac{p-5}{8}$ are integers.

$$\left(a^{\frac{p+3}{8}}\right)^2=a^{\frac{p+3}{4}}=a^{\frac{p-1}{4}}\cdot a$$

$$\left(2a(4a)^{\frac{p-5}{8}}\right)^2=2^{\frac{p-1}{2}}\cdot a^{\frac{p-1}{4}}\cdot a$$

Here $2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right)=-1 \mod p$ since $p \equiv 5 \pmod 8$.

$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)=1$ since a is QR.

So $\left(a^{\frac{p-1}{4}}\right)^2=a^{\frac{p-1}{2}} \equiv 1 \mod p$.

So $a^{\frac{p-1}{4}} \equiv \pm 1 \mod p$.

5^{68} or $10\cdot 20^{67}$ is a sol.

$5^{68} \equiv 345 \pmod{541}$ is a sol.

3. $\left(\frac{11}{1729}\right)=-1$, $11^{\frac{1729-1}{2}} \equiv 1 \mod 1729$

So 1729 is not a prime.

$1729 = 7 \times 13 \times 19$.

4. $p=a^2+5b^2 \equiv a^2 \mod 5$.

Hence $\left(\frac{p}{5}\right)=1 \Rightarrow p \equiv 1$ or $4 \pmod 5$

(Assume $p>5$)

$p=a^2+5b^2 \equiv a^2+b^2 \mod 4$.

Since $a^2 \equiv 0$ or 1, $b^2 \equiv 0$ or $1 \pmod 4$,

$p \equiv 0, 1, 2 \pmod 4$.

Since p is odd, $p \equiv 1 \mod 4$.

Hence $p \equiv 1$ or $9 \pmod{20}$.

5. $259^2+1^2=34 \times 1973$.

Choose u, v such that $u \equiv 259 \pmod{34}$

$v \equiv 1 \pmod{34}$

$-17 \le u, v \le 17$

$u=-13$, $v=1$.

Then $u^2+v^2=170=34\times 5$.

This gives $99^2+8^2=5\times 1973$.

Choose u, v such that $u \equiv 99 \pmod 5$

$v \equiv 8 \pmod 5$,

$-\frac{5}{2} \le u, v \le \frac{5}{2}$

$u=-1$, $v=2$.

Then $u^2+v^2=5$.

So $23^2+38^2=1973$.

6. $S(n)$ = # of ways to write $n = a^2+b^2$, $a \geq b \geq 0$.

If $p \equiv 1 \pmod 4$, prime, $S(p) = 1$.

We showed in the text that $S(p) \geq 1$.

Suppose $p = a^2+b^2 = c^2+d^2$

$a > b > 0$, $c > d > 0$

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

Then $a^2d^2 - b^2c^2 = d^2(p-b^2) - b^2(p-d^2)$

$= p(d^2-b^2) \equiv 0 \mod p$.

So $ad \equiv bc \pmod p$ or $ad \equiv -bc \pmod p$.

Since, $a, b, c, d < \sqrt{p}$, $ad = bc$ or $ad+bc = p$.

Here if $ad+bc = p$, $ac = bd$.

[Why? $p^2 = (a^2+b^2)(c^2+d^2) = (ad+bc)^2 + (ac-bd)^2$

$= p^2 + (ac-bd)^2$

So $ac-bd = 0$.]

Case 1. $ad = bc$. Since $\gcd(a,b) = 1$, $a \mid c$.

So $c = ak$.

So $ad = bc = bka \Rightarrow d = bk$.

$p = c^2+d^2 = k^2(a^2+b^2)$

Hence $k = 1$.

Case 2. $ac = bd$. Similar to Case 1.

$S(pq) = 2$ if p, q are distinct primes and $p, q \equiv 1 \pmod 4$

We showed that $pq = a^2+b^2$, $\gcd(a,b) = 1$ and $S(pq) \geq 2$.

We prove that the sets $\{(a,b) \,;\, n = a^2+b^2,\ a, b > 0,\ \gcd(a,b) = 1\}$ and $\{s \,;\, s^2 \equiv -1 \mod n\}$ are 1-1 correspondent.

The correspondence is ; given (a,b),

since $\gcd(a,n) = 1$,

there exists a unique $s \pmod n$ such that $as \equiv b \pmod n$.

(In other words, choose $\bar{a} \mod n$ such that $a\bar{a} \equiv 1 \mod n$.

Then $s \equiv \bar{a}b \mod n$.)

Onto ; Fermat's method of descent.

Given s, we can construct (a,b) such that $n = a^2+b^2$.

[Starting with $s^2+1 = n \cdot M$,

we can find u, v such that

$u^2+v^2 = n \cdot r$, $r < M$.

Continue this process.

1-1 ; Suppose

$n = a^2+b^2 = c^2+d^2$

and $as \equiv b$, $cs \equiv d \mod n$.

Then $ad - bc \equiv acs - asc \equiv 0 \mod n$.

Since $a, b, c, d < \sqrt{n}$, $ad = bc$.

Since $\gcd(a,b) = 1$, $a \mid c$. So $c = ak$

$\Rightarrow d = bk$.

Since $n = c^2+d^2 = k^2(a^2+b^2)$, $k = 1$.

~~A brief remark on the claim that $\gcd(ac+bd, ad-bc) = 1$ or $\gcd(ac-bd, ad+bc) = 1$~~

~~if $(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2 = (ac-bd)^2 + (ad+bc)^2$~~

~~and $\gcd(a,b) = 1$, $\gcd(c,d) = 1$.~~