Tutorial 1

Q 13

$r, m+r, 2m+r, \ldots, (n-1)m+r \qquad (r,m)=1$

$im+r \equiv jm+r \pmod{n}$

Q14

$n'' < n'$

$\sigma(n') = n'' + n'$

$\sigma(k) = 1 + k +$ stuff

Q6

$n = \prod_{i=1}^{t} p_i^{\alpha_i}$

$\phi(n) = \prod_{i=1}^{t} \phi(p_i^{\alpha_i})$

Note that $\phi(2) = 1$

$6 = 1 \cdot 6 = \cancel{2 \cdot 3}$

$\exists\ p$ st $\phi(p^t) = p^{t-1}(p-1) = 6$

If $t = 1$, $p - 1 = 6 \Rightarrow p = 7$

Otherwise $t > 1$ and $p \mid 6$

So $p = 3$ or 3

Q7

$34 = 1 \cdot 34 = \cancel{2 \cdot 17}$

$\phi(p^t) = p^{t-1}(p-1) = 34$

$\Rightarrow t > 1$ so $t \mid 34$ so $p = 2, 17$

Q5

$P_1 = 2$

$\sigma(2^k) = 1 + 2 + \dots + 2^{k-1}$ odd

If k is even, square
k odd, twice a square

Exercise

Q12, Show that $\sum_{d|n} \mu^2(d) = 2^{w(n)}$

The Möbius Function

(1) $\mu(1) = 1$

(2) If $\exists$ prime p st $p^2 | n$ then $\mu(n) = 0$

(3) Otherwise

$n = \prod_{i=1}^{t} p_i$, p_i prime , $p_i \neq p_j$, $i \neq j$

Then $\mu(n) = (-1)^t$

Theorem

Suppose f is arithmetic and define

$F(n) = \sum_{d|n} f(d)$

If f is multiplicative then so is F

Lemma

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

Proof

$$F(n) = \sum_{d|n} \mu^2(d)$$

$$F(p^k) = \sum_{d|p^k} \mu^2(d)$$

$$F(n) = \prod_{i=1}^{t}$$

Tutorial 2

Q4

a prim root

$r^{\varphi(n)} \equiv 1 \bmod (n)$

$\text{ord}_n r = \varphi(n)$

$r^d \not\equiv 1 \pmod n \qquad d < \varphi(n)$

Suppose wlog $j > i$

If $r^i \equiv r^j \pmod p$

then $r^{j-i} \equiv 1 \pmod p$

but $j - i < p - 1$

a prime root

Q8

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

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4 \end{cases}$$

<u>$p \equiv 1 \pmod 4$</u>

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$$

<u>$p \equiv 3 \pmod 4$</u>

$$\left(\frac{-3}{p}\right) = -\left(\frac{3}{p}\right)$$

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

$$\left(\frac{p}{3}\right) = \begin{cases} 1 & p \equiv 1 \pmod 3 \\ -1 & p \equiv 2 \pmod 3 \end{cases}$$

HW 4

Q5 $x = m^2 - n^2$ odd

$y = 2mn$

$z = m^2 + n^2$ odd

Q6 $m^2 + n^2 = 2mn + 1$

$m^2 - 2mn + n^2 = 1$

$(m - n)^2 = 1$

$m = n + 1$

Q10 $\left(\frac{-45}{31}\right) = \left(\frac{-1}{31}\right)\left(\frac{4}{31}\right)\left(\frac{5}{31}\right)$

$= -\left(\frac{5}{31}\right)$

$\overset{QLR}{=} -\left(\frac{31}{5}\right)$

$$= -\left(\frac{1}{5}\right)$$

$$= -1$$

Pell's Theorem

Let $d \in \mathbb{N}$, $d \neq \square^2$

Let $\frac{p_k}{q_k}$ be the kth

convergent of $\sqrt{d}$

Let t be the period length of the continued fraction expansion of $\sqrt{d}$

When t is even, the solutions of

$$x^2 - y^2 d = 1$$

p_{jt-1}, q_{jt-1}, $j \in \mathbb{N}$

and $x^2 - dy^2 = 1$ has the solutions

When this is odd the solutions of

$$x^2 - dy^2 = 1$$

are p_{2jt-1}, q_{2jt-1}, $j \in \mathbb{N}$

and the solutions of

$$x^2 - dy^2 = -1$$

are $p_{(2j-1)t-1}, q_{(2j-1)t-1}$