

# Number Theory

November 4

2014

## Congruences and properties of Congruences

Let  $a, n \in \mathbb{Z}$ , then  $n$  divides  $a$  if  $\exists b/ a = nb$ ,  $b \in \mathbb{Z}$ .  
 $n$  is a divisor of  $a$ .

**Definition.**  $p \in \mathbb{Z}$  is a **prime number** if  $p > 1$  and  $\pm 1, \pm p$  are the only divisors of  $p$ .

**Definition.**  $a, b, n \in \mathbb{Z}$ ,  $n \geq 1$ .

$a$  is **congruent to  $b$  modulo  $n$**   $\iff n \mid (a - b) \iff a - b = nk$ .

We then write:  $a \equiv b \pmod{n}$  or  $a \equiv b[n]$ .

Example:

$$-31 = -42 + 11 = (-6)7 + 11 \equiv 11[7]$$

$$a = nq + r, \quad 0 \leq r < n \quad \Rightarrow \quad a \equiv r[n]$$

$r$  is called the remainder of  $a$  divided by  $n$ .

**Theorem.**  $a, b \in \mathbb{Z}$ , then  $a \equiv b[n] \iff a$  and  $b$  have the same remainder when divided by  $n$ .

*Proof.*  $\Rightarrow$

$$\left. \begin{array}{l} a \equiv b[n] \\ a = kn + b \\ b = qn + r \end{array} \right\} \rightarrow a = qn + r + kn = (q + k)n + r$$

$\Leftarrow$

$$\left. \begin{array}{l} a = q_1n + r \\ b = q_2n + r \end{array} \right\} \Rightarrow a - b = (q_1 - q_2)n \equiv 0[n] \Rightarrow a \equiv b[n]$$

□

**Theorem.**  $n > 1$ ,  $a, b, c, d \in \mathbb{Z}$

1.  $a \equiv a[n]$

2.  $a \equiv b[n] \Rightarrow b \equiv a[n]$

3. If  $a \equiv b[n]$ ,  $b \equiv c[n]$  then  $a \equiv c[n]$

4. If  $a \equiv b[n]$ ,  $c \equiv d[n]$  then  $\begin{cases} a + c \equiv b + d[n] \\ ac \equiv bd[n] \end{cases}$

5.  $a \equiv b[n] \Rightarrow \begin{cases} a + c \equiv b + c[n] \\ ac \equiv bc[n] \end{cases}$

6.  $a \equiv b \Rightarrow a^k \equiv b^k[n]$

Example: Let's see if  $41 \mid 2^{20} - 1$ .

$$\begin{aligned} 2^{20} &= (2^5)^4 \\ 2^5 &= 32 \equiv -9[41] \\ 2^{20} &\equiv -9^4[41] \equiv 81^2 \equiv (-1)^2[41] \equiv 1[41] \\ \Rightarrow 2^{20} &\equiv 1[41] \\ \Rightarrow 2^{20} - 1 &\equiv 0[41] \end{aligned}$$

$$\begin{array}{rcl} B & 2 \cdot 4 & \equiv 2 \cdot 1[6] \\ & \not\equiv 4 & \equiv 1[6] \end{array}$$

**Theorem.**

$$ca \equiv cb[n] \Rightarrow a \equiv b\left[\frac{n}{d}\right] \quad \text{where } d = \gcd(n, c)$$

*Proof.*

$$c(a - b) = ca - cb = kn \quad k \in \mathbb{Z}$$

As

$$\begin{aligned} d = \gcd(n, c) \Rightarrow \left. \begin{array}{l} n = dr \\ c = ds \end{array} \right\} \gcd(r, s) = 1, ds(a - b) = kdr \\ s(a - b) = dr \Rightarrow r \mid s(a - b) \end{aligned}$$

But

$$\begin{aligned} \gcd(r, s) &= 1 (\Rightarrow r \nmid s) \\ \Rightarrow r \mid (a - b) &\Rightarrow a \equiv b\left[\frac{n}{b}\right] \end{aligned}$$

□

1. Corollary: If  $ca \equiv cb[n]$  and  $\gcd(n, c) = 1$ , then  $a \equiv b[n]$ .
2. Corollary: If  $ca \equiv cb[p]$ ,  $p$  prime and  $p \nmid c$ , then  $a \equiv b[p]$ .

### Chinese remainder theorem

$$\text{Let } \begin{array}{l} n_1 \dots n_r \in \mathbb{N} \\ a_1 \dots a_r \in \mathbb{Z} \end{array} \Bigg/ \gcd(n_i, n_j) = 1 \forall i \neq j$$

$$\text{then the system } \left\{ \begin{array}{lcl} x & \equiv & a_1[n_1] \\ x & \equiv & a_2[n_2] \\ \vdots & \vdots & \vdots \\ x & \equiv & a_r[n_r] \end{array} \right.$$

has a simultaneous solution which is unique modulo  $n_1 \cdot n_2 \dots n_r$

$$\Rightarrow f(x) \equiv 0[n] \text{ with } n = p_1^{k_1} \dots p_r^{k_r} \quad \left\{ \begin{array}{lcl} f(x) & \equiv & 0[p_1^{k_1}] \\ & \vdots & \\ f(x) & \equiv & 0[p_r^{k_r}] \end{array} \right.$$

*Proof.* Set

$$n = n_1 \dots n_r$$

And

$$N_k = \frac{n}{n_k} = n_1 n_2 \dots n_{k-1} n_{k+1} \dots n_r$$

Then,  $N_k x_k \equiv 1[n_k]$

$$N_k x_k + n_k y_k = 1, \text{ exists because } \gcd(N_k, n_k) = 1$$

And if we set  $\bar{x} \equiv \sum_{k=1}^r a_k N_k x_k \equiv a_k[n_k]$ , then  $\bar{x}$  is a simultaneous solution.

Uniqueness:

Suppose  $\bar{x}'$  is another solution, then for  $1 \leq k \leq r$ ,

$$\bar{x} \equiv a_k \equiv \bar{x}'[n_k]$$

$$n_k \mid (\bar{x} - \bar{x}')$$

$$\Rightarrow n_1 \dots n_r \mid (\bar{x} - \bar{x}')$$

Hence  $\bar{x}' \equiv \bar{x}[n_1 \dots n_r]$ . □

Example:

$$\left. \begin{array}{l} x \equiv 2[3] \\ x \equiv 3[5] \\ x \equiv 2[7] \end{array} \right\}$$

$$n = 3 \cdot 5 \cdot 7 = 105$$

$$N_1 = \frac{105}{3} = 35$$

$$N_2 = \frac{105}{5} = 21$$

$$N_3 = \frac{105}{7} = 15$$

That gives us the following system:

$$\left. \begin{array}{l} 35x_1 = N_1 x_1 \equiv 1[3] \\ 21x_2 = N_2 x_2 \equiv 1[5] \\ 15x_3 = N_3 x_3 \equiv 1[7] \end{array} \right\} \Rightarrow \left. \begin{array}{l} 2x_1 \equiv 1[3] \\ x_2 \equiv 1[5] \\ x_3 \equiv 1[7] \end{array} \right\} \Rightarrow \left. \begin{array}{l} x_1 = 2 \\ x_2 = 1 \\ x_3 = 1 \end{array} \right\}$$

$$\begin{aligned} \Rightarrow \bar{x} &= a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 \\ \bar{x} &= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \end{aligned}$$

## Fermat's theorem

Let  $p$  be a prime,  $a \in \mathbb{Z}/p \nmid a$ . Then,

$$a^{p-1} \equiv 1[p]$$

*Proof.* We claim that the elements in the set

$$S = \{ka \mid k = 1, 2, \dots, p-1\}$$

are all mutually incongruent modulo  $p$ . Assume that  $1 \leq k_1 < k_2 \leq p-1$  and that

$$k_1 a \equiv k_2 a[p]$$

As  $\gcd(a, p) = 1$ , we can cancel  $a$  from both sides of the equivalence, obtaining

$$k_1 \equiv k_2[p],$$

contradicting  $1 \leq k_1 < k_2 \leq p-1$ . Hence, our claim is valid.

As  $S$  contains exactly  $p-1$  elements, each one is congruent to exactly one of  $\{1, 2, \dots, p-1\}$  in some order. Hence, we have that

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1)[p]$$

and after some rearranging of the factors in the left hand side, we obtain

$$a^{p-1}(p-1)! \equiv (p-1)![p].$$

As  $\gcd(p, (p-1)!) = 1$ , we can cancel  $(p-1)!$  from both sides of the equivalence, obtaining

$$a^{p-1} \equiv 1[p]$$

□

Corollary: If  $p$  is prime, and  $a \in \mathbb{Z}$ , then

$$a^p \equiv a[p]$$

**Definition.**  $n$  is **composite** if  $n > 1$  and  $n = ab$  with  $a, b \in (1, n)$ .

**Definition.** If for some  $a \in \mathbb{Z}$ ,  $a^n \not\equiv a[n]$ , then  $n$  is not prime.  $n$  is called an **absolute pseudoprime** if  $n$  is composite and

$$a^{n-1} \equiv 1[n], \quad \forall a \in \{k \in \mathbb{Z} \mid \gcd(k, n) = 1\}$$

# Number Theory

November 7

2014

## Wilson's theorem

If  $p$  is a prime, then  $(p-1)! \equiv -1[p]$

*Proof.* Let  $a \in \{1, 2, \dots, (p-1)\}$ . Then  $\exists! a' \in \{1, 2, \dots, (p-1)\}$  such that

$$aa' \equiv 1[p]$$

If  $a = a'$  then  $a = 1$  or  $a = p-1$  because:

$$\begin{aligned} a^2 \equiv 1[p] &\iff p \mid (a^2 - 1) \\ &\Rightarrow p \mid (a+1)(a-1) \\ &\Rightarrow p \mid (a+1) \text{ or } p \mid (a-1) \\ &\Rightarrow a = 1 \text{ or } a = p-1 \end{aligned}$$

If we group all the elements remaining from  $\{2 \dots p-2\}$  into  $\frac{p-3}{2}$  pairs equal to  $1[p]$ :

$$\begin{aligned} (p-2)! &= 2 \cdot 3 \cdots (p-2) \equiv 1[p] \\ (p-1)! &\equiv -1[p] \end{aligned}$$

□

Example:  $p = 11$

$$\left. \begin{array}{l} 2 \cdot 6 \equiv 1[11] \\ 3 \cdot 4 \equiv 1[11] \\ 5 \cdot 9 \equiv 1[11] \\ 7 \cdot 8 \equiv 1[11] \end{array} \right\} 2 \cdot 6 \cdot 3 \cdot 4 \cdot 5 \cdot 9 \cdot 7 \cdot 8 = 9! \equiv 1[11]$$

And  $10! \equiv 10 \equiv -1[11]$ .

**Theorem.** Let  $p$  be an odd prime.

Then  $x^2 + 1 \equiv 0[p]$  has a solution  $\iff p \equiv 1[4]$ .

*Proof.*  $\Rightarrow$

Let  $a$  be a solution of  $a^2 \equiv -1[p]$ . We first note that  $p \nmid a$ . Raising both sides of the equivalence relation to the power  $\frac{p-1}{2}$ , we obtain

$$\begin{aligned} (a^2)^{\frac{p-1}{2}} &\equiv (-1)^{\frac{p-1}{2}}[p] \\ \Rightarrow a^{p-1} &\equiv (-1)^{\frac{p-1}{2}}[p] \end{aligned}$$

By Fermat's theorem, we have that

$$a^{p-1} \equiv 1[p]$$

which implies

$$2 \mid \frac{p-1}{2} \Rightarrow 4 \mid p-1 \Rightarrow p \equiv 1[4].$$

$\Leftarrow$

$$\begin{aligned} p &\equiv 1[4] \\ (p-1)! &= 1 \cdot 2 \cdots (p-1) \end{aligned}$$

The factors can be rearranged in the following way:

$$\begin{aligned} (p-1)! &= 1 \cdot 2 \cdots (p-2)(p-1) \\ &\equiv 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) \left(-\frac{p-1}{2}\right) \cdots (-2)(-1) \\ &= (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 [p]. \end{aligned}$$

By Wilson's theorem,

$$-1 \equiv (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 [p]$$

and as  $4 \mid p-1$ ,  $p = 4k+1$  for some  $k \in \mathbb{Z}$ , and so

$$\begin{aligned} (-1)^{\frac{p-1}{2}} &= (-1)^{\frac{4k+1-1}{2}} \\ &= 1. \end{aligned}$$

Hence,

$$-1 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 [p] \iff \left[\left(\frac{p-1}{2}\right)!\right]^2 + 1 \equiv 0[p],$$

so

$$x = \left(\frac{p-1}{2}\right)!$$

is a solution to the equation.  $\square$

Example:

$$\begin{aligned} p &= 13 \equiv 1[4] \\ \text{Set } a &= \frac{p-1}{2}! = 6! = 720 \equiv 5[13] \\ &\Rightarrow 720^2 + 1 \equiv 5^2 + 1 \equiv 26 \equiv 0[13] \end{aligned}$$

## Number Theoretic Functions

**Definition.** A function  $f$  is said to be **number theoretic** if its domain of definition is  $\mathbb{Z}^+$ .

The number theoretic functions which we will use the most are:

$$\begin{cases} \tau(n) &= \sum_{d|n} 1, \text{ the number of positive divisors of } n. \\ \sigma(n) &= \sum_{d|n} d, \text{ the sum of the positive divisors of } n. \end{cases}$$

Example: For  $n = 10$

$$\begin{aligned} \tau(10) &= 4 \\ \sigma(10) &= 1 + 2 + 5 + 10 = 18 \end{aligned}$$

**Observation:** Let  $n > 1$  with  $n = p_1^{k_1} \cdots p_r^{k_r}$  where each  $p_i$  is a distinct prime. Then the positive divisors of  $n$  are exactly

$$d = p_1^{a_1} \cdots p_r^{a_r}, \quad 0 \leq a_i \leq k_i, \quad 1 \leq i \leq r.$$

**Theorem.** Let  $n > 1$  with  $n = p_1^{k_1} \cdots p_r^{k_r}$ . Then

1.  $\tau(n) = (k_1 + 1) \cdots (k_r + 1)$
2.  $\sigma(n) = \left(\frac{p_1^{k_1+1}-1}{p_1-1}\right) \cdots \left(\frac{p_r^{k_r+1}-1}{p_r-1}\right)$

*Proof.* 1. Each  $a_i$  in  $d = p_1^{a_1} \cdots p_r^{a_r}$  can be chosen in  $(k_i + 1)$  ways. So  $a_1 \cdots a_r$  can be chosen in  $(k_r + 1) \cdots (k_1 + 1)$  ways.

2.

$$\begin{aligned} & (1 + p_1 + p_1^2 + \cdots + p_1^{k_1})(1 + p_2 + \cdots + p_2^{k_2}) \cdots (1 + p_r + \cdots + p_r^{k_r}) \\ &= \left(\frac{p_1^{k_1+1}-1}{p_1-1}\right) \cdots \left(\frac{p_r^{k_r+1}-1}{p_r-1}\right) \end{aligned}$$

□

In general we have

- $\tau(mn) \neq \tau(m)\tau(n)$
- $\sigma(mn) \neq \sigma(m)\sigma(n)$

**Definition.** A number theoretic function  $f$  is said to be **multiplicative** if

$$\gcd(m, n) = 1 \Rightarrow f(mn) = f(m)f(n)$$

Lemma : If  $\gcd(m, n) = 1$  then the divisors of  $mn$  are:

$$\mathcal{D} = \{d_1 d_2 : d_1 \mid m_1 \text{ and } d_2 \mid m_2\}$$

*Proof.* Let

$$\begin{aligned} m &= p_1^{k_1} \cdots p_r^{k_r} \\ n &= q_1^{j_1} \cdots q_s^{j_s} \\ \gcd(m, n) &= 1 \end{aligned}$$

Then  $\forall i, j, q_i \neq p_i$ , so if  $d \mid mn$ , then

$$d = \underbrace{p_1^{a_1} \cdots p_r^{a_r}}_{d_1} \underbrace{q_1^{b_1} \cdots q_s^{b_s}}_{d_2}$$

where  $d_1 \mid m_1$  and  $d_2 \mid m_2$ . Thus,  $d \in \mathcal{D}$ .  $\square$

**Theorem.** Let  $f$  be a multiplicative number theoretic function and define  $F(n)$  by:

$$F(n) = \sum_{d \mid n} f(d), \quad n \geq 1$$

Then  $F$  is also a multiplicative number theoretic function.

*Proof.* Assume  $\gcd(m, n) = 1$ . Then

$$\begin{aligned} F(m, n) &= \sum_{d \mid mn} f(d) = \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1 d_2) = \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1) f(d_2) = \sum_{d_1 \mid m} f(d_1) \sum_{d_2 \mid n} f(d_2) \\ &= F(m) F(n) \end{aligned} \quad \square$$

Corollary :  $\sigma$  and  $\tau$  are multiplicative:

$$\begin{aligned} \text{Write } \tau(n) &= \sum_{d \mid n} 1 = \sum_{d \mid n} f(d) && \text{with } f(d) = 1 \\ \sigma(n) &= \sum_{d \mid n} d = \sum_{d \mid n} g(d) && \text{with } g(d) = d \end{aligned}$$



# Number Theory

November 11

2014

**Definition.** The Möbius function  $\mu$  is defined by:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } \exists p \text{ prime such that } p^2 \mid n \\ (-1)^r & \text{if } n = p_1 p_2 \dots p_r, \text{ with distinct primes.} \end{cases}$$

Example:

$$\begin{aligned} \mu(6) &= (-1)^2 & 6 &= 2 \cdot 3 \\ \mu(12) &= 0 & 12 &= 2^2 \cdot 3 \end{aligned}$$

**Theorem.**  $\mu$  is multiplicative.

*Proof.* Let  $\gcd(m, n) = 1$  and assume  $p^2 \mid m$  or  $p^2 \mid n$ , with  $p$  prime. Without loss of generality, say  $p^2 \mid m$ . Then

$$\begin{aligned} \mu(mn) &= \mu(p^2 q) \\ &= 0 \\ &= 0 \cdot \mu(n) \\ &= \mu(m)\mu(n) \end{aligned}$$

and we are done. Now let  $m > 1$  and  $n > 1$  both be square free:

$$\begin{aligned} m &= p_1 p_2 \dots p_r \\ n &= q_1 q_2 \dots q_s \end{aligned}$$

with  $p_i, q_j$  distinct primes. Then:

$$\mu(m, n) = (-1)^{r+s} = (-1)^r (-1)^s = \mu(m)\mu(n)$$

The cases when exactly one or both of  $m$  and  $n$  equals 1 are left to the reader.  $\square$

**Theorem.** For  $n \geq 1$ ,

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$$

*Proof.* Set  $F(n) = \sum_{d \mid n} \mu(d)$ . As  $\mu$  is multiplicative, so is  $F$ . For  $n = 1$  we have

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

Assume  $n > 1$ ,  $n = p_1^{k_1} \dots p_r^{k_r}$ , with  $p_i$  distinct primes. For any prime  $p$ , we have that

$$\begin{aligned} F(p^k) &= \sum_{d|p^k} \mu(d) \\ &= \mu(1) + \mu(p) + \mu(p^2) + \dots + \mu(p^k) \\ &= 1 - 1 + 0 + 0 + \dots + 0 \\ &= 0 \end{aligned}$$

and by multiplicity,

$$\begin{aligned} F(n) &= F(p_1^{k_1}) \dots F(p_r^{k_r}) \\ &= 0. \end{aligned}$$

□

## Möbius inversion formula

Let  $F$  and  $f$  be connected by

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

Then

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$$

*Proof.* We first show that the two sums are indeed equal. Set  $d' = \frac{n}{d}$ . As  $d$  ranges over all the divisors of  $n$ , so does  $d'$ . Thus,

$$\begin{aligned} \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) &= \sum_{d|n} \mu\left(\frac{n}{d'}\right) F(d') \\ &= \sum_{d'|n} \mu\left(\frac{n}{d'}\right) F(d') \end{aligned}$$

Furthermore, we have

$$\begin{aligned} \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) &= \sum_{d|n} \left( \mu(d) \sum_{c|\frac{n}{d}} f(c) \right) \\ &= \sum_{d|n} \left( \sum_{c|\frac{n}{d}} \mu(d) f(c) \right) \end{aligned} \tag{1}$$

We note that

$$d \mid n \wedge c \mid \frac{n}{d} \quad \Leftrightarrow \quad c \mid n \wedge d \mid \frac{n}{c}$$

Thus, we can rewrite (1) as follows

$$\begin{aligned} \sum_{d|n} \left( \sum_{c|\frac{n}{d}} \mu(d) f(c) \right) &= \sum_{c|n} \left( \sum_{d|\frac{n}{c}} \mu(d) f(c) \right) \\ &= \sum_{c|n} \left( f(c) \sum_{d|\frac{n}{c}} \mu(d) \right) \end{aligned} \quad (2)$$

As by our previous theorem,

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

the last sum in (2) reduces to

$$\begin{aligned} \sum_{c=n} \left( f(c) \sum_{d|\frac{n}{c}} \mu(d) \right) &= \sum_{c=n} f(c) \cdot 1 \\ &= f(n) \end{aligned}$$

□

Example:

$$\sigma(n) = \sum_{c|n} c; \quad f(n) = n$$

Möbius inverse:

$$n = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sigma(d)$$

**Theorem.** Let  $f, F$  be connected by:

$$F(n) = \sum_{d|n} f(d); \quad \text{if } F \text{ is multiplicative, then } f \text{ is multiplicative}$$

*Proof.* Let  $\gcd(m, n) = 1$ . Then

$$\begin{aligned} f(mn) &= \sum_{d|mn} \mu(d) F\left(\frac{mn}{d}\right) \\ &= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1 d_2) F\left(\frac{m}{d_1} \frac{n}{d_2}\right) \\ &= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1) \mu(d_2) F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right) \\ &= \left( \sum_{d_1|m} \mu(d_1) F\left(\frac{m}{d_1}\right) \right) \left( \sum_{d_2|n} \mu(d_2) F\left(\frac{n}{d_2}\right) \right) \\ &= f(n) f(m) \end{aligned}$$

□

## Euler's $\varphi$ function

For  $n \geq 1$  Euler's  $\varphi$  function is defined as  $\varphi(n)$  = the number of integers in  $\{1, 2, \dots, n\}$  that are relatively prime to  $n$ . In other words,

$$\varphi(n) = |\{a \in \mathbb{Z} : 1 \leq a \leq n, \gcd(a, n) = 1\}|$$

Example: Let  $n = 18$ . Then  $\{a \in \mathbb{Z} : 1 \leq a \leq n, \gcd(a, n) = 1\} = \{1, 5, 7, 11, 13, 17\}$ , so  $\varphi(18) = 6$

**Theorem.** For  $p$  prime,  $k > 0$ :

$$\varphi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$$

*Proof.*

$$\gcd(n, p^k) = 1 \iff p \nmid n$$

The multiples of  $p$  in  $[1, p^k]$  are  $p, 2p, \dots, pp, \dots, p^{k-1}p$ , adding up to  $p^{k-1}$  numbers.

Hence

$$\varphi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$$

□

**Lemma :** For  $a, b, c \in \mathbb{Z}$ ,  $\gcd(a, bc) = 1 \iff \gcd(a, b) = 1 = \gcd(a, c)$ .

*Proof.*  $\Rightarrow$  Trivial.

$\Leftarrow$  Each prime factor in  $a$  is distinct from every prime factor in  $b$  and in  $c$ . Hence  $\gcd(a, bc) = 1$ . □

**Theorem.**  $\varphi$  is multiplicative.

*Proof.* Let  $m, n \in \mathbb{Z}$  with  $\gcd(m, n) = 1$ . Since  $\varphi(1) = 1$ , the result holds when  $m = 1$  or  $n = 1$ .

Let  $m > 1, n > 1$  and construct a table consisting of all numbers  $1, \dots, mn$  in the following way

$$\begin{array}{ccccccc} & 1 & & 2 & \cdots & & r & \cdots & m \\ m+1 & & & m+2 & & & m+r & & 2m \\ 2m+1 & & & 2m+2 & & & 2m+r & & 3m \\ & \vdots & & \vdots & & & \vdots & & \vdots \\ (n-1)m+1 & & & (n-1)m+2 & & & (n-1)m+r & & nm \end{array} \quad (3)$$

We know that  $\varphi(mn)$  is equal to the number of entries in the table which are relatively prime to  $mn$  and by our previous lemma, this is the same as the number of entries which are relatively prime to both  $m$  and  $n$ .

We note that  $\gcd(qm + r, m) = \gcd(r, m)$ , so the numbers in the  $r$ th column

are relatively prime to  $m$  if and only if  $\gcd(r, m) = 1$ . Hence, there are  $\varphi(m)$  columns of numbers relatively prime to  $m$ . If we can show that there are  $\varphi(n)$  numbers in each such column which are relatively prime to  $n$  we are done. Assume that  $\gcd(r, m) = 1$ . Consider the set of  $n$  integers in the  $r$ th column

$$R = \{km + r : k = 0, \dots, (n-1)\}$$

We claim that these are pairwise incongruent modulo  $n$ . Assume that  $0 \leq k_1 < k_2 \leq n-1$  and that

$$k_1m + r \equiv k_2m + r \pmod{n}$$

Subtracting  $r$  and canceling  $m$  from both sides of the equation results in

$$k_1 \equiv k_2 \pmod{n},$$

which is a contradiction. Thus, our claim holds and the numbers in  $R$  are congruent modulo  $n$  to  $0, 1, \dots, n-1$  in some order.

We note that if  $s \equiv t \pmod{n}$  and  $\gcd(s, n) = 1$ , then  $\gcd(t, n) = 1$ . Hence, the number of integers in  $R$  relatively prime to  $n$  are  $\varphi(n)$ , which is what we wanted to show.  $\square$

**Theorem.** For  $n = p_1^{k_1} \dots p_r^{k_r}$ ;  $\varphi(n) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_r})$

*Proof.*

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{k_1}) \dots \varphi(p_r^{k_r}) \\ &= p_1^{k_1} (1 - \frac{1}{p_1}) \dots p_r^{k_r} (1 - \frac{1}{p_r}) \\ &= n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_r}) \end{aligned}$$

$\square$

Example :  $\varphi(18) = \varphi(2 \cdot 3^2) = 18(1 - \frac{1}{2})(1 - \frac{1}{3}) = 18 \cdot \frac{1}{2} \cdot \frac{2}{3} = 6$

# Number Theory

November xx

2014

Lemma : Let  $n > 1$ , and  $\gcd(a, n) = 1$ . If

$$a_1, \dots, a_{\varphi(n)} \in [1, n)$$

are the positive integers which are relatively prime to  $n$ , then

$$aa_1, \dots, aa_{\varphi(n)}$$

are congruent to  $a_1, \dots, a_{\varphi(n)}$  modulo  $n$  in some order.

*Proof.* We claim that the  $aa_i$ s are pairwise incongruent modulo  $n$ . Assume that

$$aa_i \equiv aa_j[n], \quad i < j.$$

Since  $\gcd(a, n) = 1$ ,  $a_i \equiv a_j[n] \Rightarrow a_i = a_j \Rightarrow i = j$ .

As  $\gcd(a, n) = 1$  and  $\gcd(a_i, n) = 1$ , we have that  $\gcd(aa_i, n) = 1$ . Let

$$aa_i \equiv b[n].$$

Then

$$1 = \gcd(aa_i, n) = \gcd(b, n),$$

so  $b = a_j$  for some  $j$ . □

## Euler's theorem

Let  $n > 1$  and  $\gcd(a, n) = 1$ . Then

$$a^{\varphi(n)} \equiv 1[n]$$

*Proof.* Let  $a_1, \dots, a_{\varphi(n)}$  be as in our previous lemma and write

$$\begin{cases} aa_1 & \equiv & a'_1[n] \\ & \vdots & \\ aa_{\varphi(n)} & \equiv & a'_{\varphi(n)}[n] \end{cases}$$

so that after permutation,

$$\{a'_1, \dots, a'_{\varphi(n)}\} = \{a_1, \dots, a_{\varphi(n)}\}.$$

We have that

$$(aa_1) \cdots (aa_{\varphi(n)}) \equiv a'_1 \cdots a'_{\varphi(n)} = a_1 \cdots a_{\varphi(n)}[n]$$

implying that

$$a^{\varphi(n)}(a_1 \cdots a_{\varphi(n)}) \equiv 1 \cdot (a_1 \cdots a_{\varphi(n)})[n].$$

As for each  $i$ ,  $\gcd(a_i, n) = 1$ ,  $\gcd(a_1 \cdots a_{\varphi(n)}, n) = 1$ . Thus we can cancel the factors and obtain

$$a^{\varphi(n)} \equiv 1[n],$$

which is what we wanted to show.  $\square$

Lemma : For  $n \geq 1$ , let

$$S_d = \{m : 1 \leq m \leq n, \gcd(m, n) = d\}.$$

Then

$$\{1, 2, \dots, n\} = \bigcup_{d|n} S_d$$

and the union is disjoint.

*Proof.*  $\subseteq$ :

Let  $k \in \{1, 2, \dots, n\}$  and  $\gcd(k, n) = b$ . Then  $b \mid n$ , so

$$k \in S_b \subset \bigcup_{d|n} S_d.$$

Thus,  $\{1, 2, \dots, n\} \subseteq \bigcup_{d|n} S_d$ .

$\supseteq$ : Trivial.

Thus,

$$\{1, 2, \dots, n\} = \bigcup_{d|n} S_d$$

Assume  $k \in S_{d_1} \cap S_{d_2}$ , with  $d_1 \neq d_2$ . Then

$$\gcd(k, n) = d_1 \neq d_2 = \gcd(k, n)$$

which is a contradiction. Thus, the union is disjoint.  $\square$

## Gauss' theorem

For  $n \geq 1$ ,

$$\sum_{d|n} \varphi(d) = n$$

*Proof.* Let  $S_d$  be as in our previous lemma. By the lemma, we have

$$n = \sum_{d|n} |S_d|$$

Furthermore, we have that

$$\begin{aligned} S_d &= \left\{ d \frac{m}{d} : 1 \leq \frac{m}{d} \leq \frac{n}{d}, \quad \gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1 \right\} \\ &= \left\{ m' : 1 \leq m' \leq \frac{n}{d}, \quad \gcd\left(m', \frac{n}{d}\right) = 1 \right\}. \end{aligned}$$

Thus,

$$|S_d| = \varphi\left(\frac{n}{d}\right)$$

and so,

$$\begin{aligned} n &= \sum_{d|n} |S_d| \\ &= \sum_{d|n} \varphi\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \varphi(d), \end{aligned}$$

which is what we wanted to show.  $\square$

Example:  $n = 10$

$$\begin{aligned} S_1 &= \{1, 3, 7, 9\} & |S_1| &= 4 = \varphi\left(\frac{10}{1}\right) \\ S_2 &= \{2, 4, 6, 8\} & |S_2| &= 4 = \varphi\left(\frac{10}{2}\right) \\ S_5 &= \{5\} & |S_5| &= 1 = \varphi\left(\frac{10}{5}\right) \\ S_{10} &= \{10\} & |S_{10}| &= 1 = \varphi\left(\frac{10}{10}\right) \end{aligned}$$

and  $10 = \varphi(10) + \varphi(5) + \varphi(2) + \varphi(1)$ .

**Corollary:**  $\varphi$  is multiplicative.

*Proof.* Set  $F(n) = n$ . Then

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

and

$$F \text{ multiplicative} \Rightarrow \varphi \text{ multiplicative.}$$

$\square$



**Theorem.** For  $n \geq 1$ ,

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$$

*Proof.* From

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

Möbius inversion formula implies

$$\begin{aligned} \varphi(n) &= \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \mu(d) \frac{n}{d} \\ &= n \sum_{d|n} \frac{\mu(d)}{d}. \end{aligned}$$

□

We have previously shown that for  $n > 1$ ,

$$\varphi(n) = n \prod_{p_i|n} \left(1 - \frac{1}{p_i}\right)$$

and using the last theorem, we can obtain this result using a different reasoning. Let  $n = p_1^{k_1} \cdots p_r^{k_r}$  be the prime factorization of  $n$ . Now consider the product

$$P = \prod_{p_i|n} \left( \mu(1) + \frac{\mu(p_i)}{p_i} + \cdots + \frac{\mu(p_i^{k_i})}{p_i^{k_i}} \right).$$

Expanding this product yields a sum of terms on the form

$$\frac{\mu(1)\mu(p_1^{a_1})\mu(p_2^{a_2})\cdots\mu(p_r^{a_r})}{p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}} \quad 0 \leq a_i \leq k_i \quad (4)$$

and as  $\mu$  is multiplicative, (4) can be rewritten as

$$\frac{\mu(p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r})}{p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}} = \frac{\mu(d)}{d}.$$

Thus,  $P = \sum_{d|n} \frac{\mu(d)}{d}$  and by our previous theorem

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d} = n \prod_{p_i|n} \left( \mu(1) + \frac{\mu(p_i)}{p_i} + \cdots + \frac{\mu(p_i^{k_i})}{p_i^{k_i}} \right)$$

and since  $\mu(p_i^{a_i}) = 0$  for  $a_i \geq 2$ ,

$$\varphi(n) = n \prod_{p_i|n} \left( \mu(1) + \frac{\mu(p_i)}{p_i} \right) = n \prod_{p_i|n} \left( 1 - \frac{1}{p_i} \right).$$

# Number Theory

November 18

2014

**Definition.** The *order* of  $a[n]$  is the smallest positive integer  $k$  such that

$$a^k \equiv 1[n]$$

We write  $k = \text{ord}_n(a)$

Example:  $a = 2, n = 7$

$$2^3 = 8 \equiv 1[7]$$

$$2^1 \equiv 2, 2^2 = 4 \equiv 1[7]$$

**Theorem.** Let  $\text{ord}_n(a) = k$ , then:

$$a^n \equiv 1[n] \iff k \mid n$$

In particular,  $k \mid \varphi(n)$

*Proof.*  $\Leftarrow$

$$n = qk, \quad q \in \mathbb{Z}$$

$$a^n = (a^k)^q \equiv 1^q \equiv 1[n]$$

$\Rightarrow$

$$n = qk + r, \quad 0 \leq r < k$$

$$1 \equiv a^n \equiv (a^k)^q a^r \equiv a^r[n]$$

Now if  $r = 0$ ,  $n = qk$ , then  $k \mid n$  and we are done. If  $r \neq 0$ , then this contradicts  $\text{ord}_n(a) = k$ , as  $0 < r < k$  and the result follows.

Lastly, Euler's theorem implies  $a^{\varphi(n)} \equiv 1[n]$ , and so  $k \mid \varphi(n)$ .  $\square$

Example:  $k = \text{ord}_{11}(2) \quad 2^{10} \equiv 1[11]$

$$k \mid 10 \Rightarrow k \in \{1, 2, 5, 10\}$$

If  $k =$

$$1 : 2^1 = 2 \not\equiv 1[11]$$

$$2 : 2^2 = 4 \not\equiv 1[11]$$

$$5 : 2^5 = 32 \equiv -1 \not\equiv 1[11]$$

Hence  $\text{ord}_{11}(2) = 10$

**Theorem.** Let  $\text{ord}_n(a) = k$ , then:

$$\begin{aligned} a^i &\equiv a^j[n] \\ \iff i &\equiv j[k] \end{aligned}$$

*Proof.*  $\Rightarrow$   
Say  $i \leq j$

$$\begin{aligned} a^i &\equiv a^j \equiv a^{i+(j-i)} \equiv a^i a^{j-i}[n] \\ \gcd(a^i, n) &= 1, \quad 1 \equiv a^{j-i}[n] \end{aligned}$$

The precedent theorem says:

$$k \mid j - i \Rightarrow j \equiv i[k]$$

$\Leftarrow$

$$\begin{aligned} j &= qk + i \\ a^j &= a^{qk+i} = \underbrace{(a^k)^q}_{\equiv 1} a^i \equiv a^i[n] \end{aligned}$$

□

**Corollary:** Let  $\text{ord}_n(a) = k$ ,  
then  $a^1, a^2, \dots, a^k$  are incongruent modulo  $n$ .

*Proof.* Assume  $1 \leq j \leq i \leq k$

$$a^i \equiv a^j[n]$$

The previous theorem implies:

$$\begin{aligned} i &\equiv j[k] \\ i &= j \end{aligned}$$

□

**Theorem.** Let  $\text{ord}_n(a) = k, h > 0$   
Then  $a^h$  has order  $\text{ord}_n(a^h) = \frac{k}{\gcd(h, k)}$

*Proof.* Set  $d = \gcd(h, k)$

$$\begin{aligned} h &= h_1 d \\ k &= k_1 d \quad \text{and} \quad \gcd(h_1, k_1) = 1 \end{aligned}$$

Then:

$$(a^h)^{k_1} = a^{\frac{hk_1}{d}} = a^{kh_1} \equiv 1^{h_1} \equiv 1[n]$$

Now set  $r = \text{ord}_n(a^h), r \mid k_1$

$$\begin{aligned} a^{hr} &= (a^h)^r \equiv 1[n] \\ k \mid hr &\Rightarrow \frac{hr}{k} \in \mathbb{Z} \Rightarrow \frac{\frac{h}{d}r}{\frac{k}{d}} \in \mathbb{Z} \Rightarrow \frac{h_1 r}{k_1} \in \mathbb{Z} \Rightarrow k_1 \mid h_1 r \end{aligned}$$

Euclid's lemma implies:

$$k_1 \mid r \Rightarrow r = k_1$$

$$\text{ord}_n(a^h) = r = k_1 = \frac{k}{d} = \frac{k}{\gcd(h, k)}$$

□

Example:  $n = 7, a = 3$

$$3^2 = 9 \equiv 2 \pmod{7}$$

$$3^3 = 27 \equiv -1 \pmod{7}$$

$$\Rightarrow k = \text{ord}_7(3) = 6$$

If  $h = 2$ ,

$$\text{ord}_7(3^2) = \frac{6}{\gcd(2, 6)} = \frac{6}{2} = 3$$

$$\text{So } \text{ord}_7(2) = 3 \Rightarrow 2^3 \equiv 1 \pmod{7}$$

Remark: if  $a \equiv b \pmod{n}$

$$\begin{aligned} b^k &\equiv a^k \equiv 1 \pmod{n} \\ b^j &\equiv a^j \equiv 1 \pmod{n} \end{aligned} \quad \text{with } 1 \leq j \leq k-1$$

$$\Rightarrow \text{ord}_n(b) = \text{ord}_n(a)$$

**Definition.**  $a$  is called a **primitive root modulo  $n$**  if  $\text{ord}_n(a) = \varphi(n)$

Example: 3 is a primitive root modulo 7:  $\text{ord}_7(3) = 6 = 7 - 1 = \varphi(7)$

Lagrange's theorem: Let  $p$  be a prime, and  $f$  such that:

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

$$a_i \in \mathbb{Z}$$

$$a_n \not\equiv 0 \pmod{p}$$

Then  $f(x) \equiv 0 \pmod{p}$  has at most  $n$  incongruent solutions.

*Proof.* by induction on  $n$ . At  $n=1$ :

$$\begin{aligned} f(x) &= a_1 x + a_0 \equiv 0 \pmod{p} \\ \Rightarrow a_1 x &\equiv -a_0 \pmod{p} \\ \gcd(a_1, p) &= 1 \\ \Rightarrow &\text{there exist a unique solution modulo } p \end{aligned}$$

Now assume it is true for polynomials of some degree  $k-1$  and let  $\deg(f(x)) = k$ . If  $f(x) \equiv 0 \pmod{p}$  has no solution, we're done. If such a solution  $x = a$  exists,

$$f(a) \equiv 0 \pmod{p}$$

$$f(x) = (x - a)q(x) + r, \quad q(x) \in \mathbb{Z}[X], r \in \mathbb{Z}$$

Since  $\deg(q(x)) = k - 1$

$$0 \equiv f(a) \equiv (a - a)q(a) + r = r[p]$$

Ergo  $r \equiv 0[p]$

$$\Rightarrow f(x) = (x - a)q(x)$$

Now suppose  $b \neq a$  is another solution to  $f(x) \equiv 0[p]$ .

$$0 \equiv f(b) \equiv (b - a)q(b)[p]$$

$$p \mid (b - a)q(b)$$

$$b \neq a \Rightarrow p \mid q(b) \Rightarrow q(b) \equiv 0[p]$$

Since  $q(x) \equiv 0[p]$  has less or equal than  $k - 1$  incongruent solutions, we get that  $f(x) \equiv 0[p]$  has less or equal than  $1 + (k - 1) = k$  incongruent solutions modulo  $p$ .  $\square$

**Corollary:** For  $p$  prime,  $d \mid p - 1$ :

$$x^d - 1 \equiv 0[p]$$

has exactly  $d$  incongruent solutions.

*Proof.* Let  $p - 1 = dk$

Then

$$x^{p-1} - 1 = (x^d - 1) \underbrace{(x^{d(k-1)} + \dots + x^{2d} + x^d + 1)}_{f(x)}$$

Fermat's theorem implies:  $x^{p-1} - 1 \equiv 0[p]$  has  $p - 1$  solutions, and

Lagrange's theorem implies:  $f(x) \equiv 0[p]$  has less or equal than  $d(k - 1) = p - 1 - d$  solutions. Set  $a$  a solution of  $x^{p-1} - 1 \equiv 0[p]$ :

$$0 \equiv a^{p-1} - 1 = (a^d - 1)f(a)[p]$$

$$p \mid (a^d - 1) \quad \text{or} \quad p \mid f(a)$$

$$\Rightarrow a \text{ is a solution of } x^d - 1 \equiv 0[p]$$

And by using Lagrange's theorem:

$$\left. \begin{array}{l} x^d - 1 \equiv 0[p] \text{ has over or equal to } d \text{ incongruent solutions}[p] \\ x^d - 1 \equiv 0[p] \text{ has less or equal than } d \text{ incongruent solutions}[p] \end{array} \right\} d \text{ solutions.}$$

$\square$

**Theorem.** Let  $p$  be a prime,  $d \mid p - 1$ , then there are exactly  $\varphi(d)$  incongruent integers of order  $d$  modulo  $p$ .

*Proof.* For  $d \mid \overbrace{(p-1)}^{=\varphi(p)}$ , set  $\psi(d)$  the number of  $a \leq p-1$  of order  $p$ .

$$\Rightarrow p-1 = \sum_{d \mid (p-1)} \psi(d)$$

For  $d \mid p-1$

$$d = \sum_{c \mid d} \psi(c) ;$$

And there are by the corollary exactly  $d$  incongruent solutions  $a_1, \dots, a_d$  to  $x^d - 1 \equiv 0[p]$ .

Then  $a_i^d \equiv 1[p]$ .

So  $c = \text{ord}_p(a_i) \mid d$  And if , for some  $b \leq p-1$ ,

$$c = \text{ord}_p(b) \mid d$$

$$1 \equiv b^c \Rightarrow (b^c)^{dk} \equiv b \equiv 1[p] \Rightarrow b \in \{a_1 \dots a_d\}$$

By Möbius inversion formula:

$$\Rightarrow \psi(d) = \sum_{c \mid d} \mu(c) \frac{d}{c} = \varphi(c)$$

□

Illustration:  $p = 11$

$a$	$\text{ord}_1 1(a)$	
1	1	
2	10	
3	5	
4	5	
5	5	
6	10	
7	10	
8	10	
9	5	
10	2	

$$\left. \begin{array}{l} \psi(1) = 1 = \varphi(1) \\ \psi(2) = 1 = \varphi(2) \\ \psi(5) = 4 = \varphi(5) \\ \psi(10) = 1 = \varphi(10) \end{array} \right\} 10 = 4 + 4 + 1 + 1$$

**Corollary:** A prime  $p$  has exactly  $\varphi(p-1)$  primitive elements  
(This is the case  $d = p-1$  of the precedent theorem)

Application:  $p \equiv 1[4] \Rightarrow x^2 \equiv -1[p]$  has a solution.

Take  $d = 4$  in the theorem:  $4 \mid p-1$

Then there exists an  $a$  of order 4 modulo  $p$ .

$$p \mid (a^4 - 1) = (a^2 - 1)(a^2 + 1)$$

$$p \mid a^2 - 1 \text{ or } p \mid a^2 + 1$$

$$\Rightarrow \left. \begin{array}{l} a^2 \equiv 1[p] \\ a^2 \equiv -1[p] \end{array} \right\} x = a \text{ is a solution to } x^2 \equiv -1[p]$$

# Number Theory

November 19

2014

Lemma:  $p$  an odd prime, there is a primitive element  $r[p]$  such that:

$$r^{p-1} \not\equiv 1[p^2]$$

*Proof.* Let  $r$  be a primitive root modulo  $p$ .

- If  $r^{p-1} \not\equiv 1[p^2]$ , we're done.
- If  $r^{p-1} \equiv 1[p^2]$ , set  $r' = r + p$ ,  $\text{ord}_p(r) = \text{ord}_p(r') = p - 1$

$$\begin{aligned} r'^{p-1} &= (r+p)^{p-1} \equiv r^{p-1} + \underbrace{\binom{p-1}{1} r^{p-2} p}_{p-1} [p^2] \\ &= r^{p-1} + p^2 r^{p-2} - r^{p-2} p \\ &\equiv 1 - r^{p-2} p \equiv 1[p^2] \text{ since } p \nmid r \end{aligned}$$

□

Lemma: Let  $r$  be a primitive root modulo  $p$  such that:

$$r^{p-1} \equiv 1[p^2]$$

Then for each  $k \geq 2$ ,

$$\begin{aligned} r^{p^{k-2}(p-1)} &\not\equiv 1[p^k] \\ p^{k-2}(p-1) &= \frac{p^{k-1}(p-1)}{p} = \frac{\varphi(p^k)}{p} \end{aligned}$$

*Proof.* Induction on  $k \geq 2$

Case  $k = 2$  is the assumption. Now assume for a particular  $k$ :

$$\begin{aligned} r^{p^{k-2}(p-1)} &= r^{\varphi(p^{k-1})} \equiv 1[p^{k-1}] \\ r^{p^{k-2}(p-1)} &= 1 + ap^{k-1} \quad a \in \mathbb{Z} \quad p \nmid a \end{aligned}$$

At  $k + 1$ :

$$\begin{aligned} r^{p^{k-1}(p-1)} &= (r^{p^{k-2}(p-1)})^p \equiv (1 + ap^{k-1})^p \\ &\equiv 1 + \binom{p}{1} ap^{k-1} + \underbrace{\binom{p}{2} a^2 p^{2(k-1)} + \dots}_{=0} \\ &\equiv 1 + ap^k [p^{k+1}] \\ &\not\equiv 1[p^{k+1}] \end{aligned}$$

□

**Theorem.**  $k \geq 1$ ,  $\forall p$  odd prime,  $\exists r[p^k]$  a primitive root.

*Proof.* Take  $r$  a primitive root modulo  $p$ . We assume from a precedent lemma that  $r^{p^{k-2}(p-1)} \not\equiv 1[p^k]$  Set  $n = \text{ord}_{p^k}(r)$ , then

$$\begin{aligned} r^n &\equiv 1[p] \Rightarrow (p-1) \mid n \\ n \mid \varphi(p^k) &= p^{k-1}(p-1) \\ \Rightarrow n &= p^m(p-1), \quad 0 \leq m \leq k-1 \end{aligned}$$

- If  $m = k-1$  it's done,  $r$  is a primitive root.
- If  $m \leq k-2$ :

$$r^{p^{k-2}(p-1)} = r^{p^m(p-1)p^{(k-2)-m}} \equiv 1[p^k] : \text{absurd!}$$

□

**Definition.** For  $\gcd(a, n) = 1$ , the *index* of  $a$  in the base  $r$  is the smallest positive integer  $h$  such that:

$$\begin{aligned} a &\equiv r^h[n] \\ \text{ind}_r(a) &= h \end{aligned}$$

If  $a \equiv b[n]$  then  $\text{ind}(a) = \text{ind}(b)$

**Theorem.**  $n, r$  as above.

- a)  $\text{ind}_r(a, b) \equiv \text{ind}_r(a) + \text{ind}_r(b)[\varphi(n)]$
- b)  $\text{ind}_r(a^k) \equiv k \cdot \text{ind}_r(a)[\varphi(n)]$
- c)  $\text{ind}_r(1) \equiv 0$
- d)  $\text{ind}_r(r) \equiv 1[\varphi(n)]$



# Number Theory

November 21

2014

In a polynomial equation, we always state  $p \nmid a$ , since  $ax^2 + bx + c \equiv 0[p] \iff bx + c \equiv 0[p]$  if it does. To introduce the quadratic residue, we will try to prove that

$$x^2 \equiv a[p], p \text{ an odd prime}$$

has either 0 or 2 incongruent solutions. Let's suppose  $x_0$  is a solution, then  $-x_0$  is another:

$$(-x_0)^2 \equiv x_0^2 \equiv a[p]$$

$$\text{If } x_0 \equiv -x_0[p]$$

$$\Rightarrow 2x_0 \equiv 0[p]$$

$$\Rightarrow p \mid x_0$$

$$\Rightarrow p \mid a : \text{absurd!}$$

$$\Rightarrow x_0 \not\equiv -x_0[p]$$

Hence, there are at least 2 solutions. But we also know by Lagrange's theorem that:  $\deg(x^2 - 2) = 2 \Rightarrow$  there are 2 or less incongruent solutions. Therefore, there are exactly 2 solutions.

**Definition.**  $p$  an odd prime,  $p \nmid a$ .  $a$  is called a quadratic residue modulo  $p$  if

$$x^2 \equiv a[p] \text{ has 2 incongruent solutions}$$

$a$  is called a quadratic non residue if the equation has no solution.

Example:  $p = 11$

$$\left. \begin{array}{l} 1^2 \equiv 10^2 \equiv 1 \\ 2^2 \equiv 9^2 \equiv 4 \\ 3^2 \equiv 8^2 \equiv 9 \\ 4^2 \equiv 7^2 \equiv 5 \\ 5^2 \equiv 6^2 \equiv 3 \end{array} \right\} [11]$$

1, 3, 4, 5, 9 are quadratic residues, and 2, 6, 7, 8, 10 are quadratic non residues [11].

**Euler's criterion:** Let  $p$  be an odd prime, and  $p \nmid a$ .

Then  $a$  is a quadratic residue iff:

$$a^{\frac{p-1}{2}} \equiv 1[p]$$

*Proof.* :

$\Rightarrow$  Let  $x_1$  be such that  $x_1^2 \equiv a[p]$

$$a^{\frac{p-1}{2}} \equiv (x_1^2)^{\frac{p-1}{2}} = x_1^{p-1} \underbrace{\equiv 1[p]}_{\text{Fermat's thm}}$$

$\Leftarrow$  Assume  $a^{\frac{p-1}{2}} \equiv 1[p]$

Fix a primitive root  $r[p]$  and

$$\begin{aligned} a &\equiv r^k[p], \quad k = \text{ind}_p(a) \\ 1 &\equiv a^{\frac{p-1}{2}} \equiv (r^k)^{\frac{p-1}{2}} = r^{\frac{k(p-1)}{2}}[p] \\ \text{ord}_p(r) &= (p-1) \mid \frac{k(p-1)}{2} \end{aligned}$$

Therefore  $\exists \ell \in \mathbb{Z} / \frac{k(p-1)}{2} = (p-1)\ell \implies k = 2\ell$  is even and  $a = r^k = r^{2\ell}[p]$  is a quadric residue!  $\square$

"Extra argument"

$$\begin{aligned} a^{p-1} &\equiv 1[p] \\ p \mid (a^{p-1} - 1) &= (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \\ \Rightarrow a^{\frac{p-1}{2}} &\equiv \pm 1[p] \end{aligned}$$

Hence  $a$  is a quadric non residue iff  $a^{\frac{p-1}{2}} \equiv -1[p]$

**Definition.**  $p$  an odd prime,  $p \nmid a$ .

The **Lagrange symbol** is defined by:

$$(a/p) = \begin{cases} 1 & \text{if } a \text{ is a quadric residue mod } p \\ -1 & \text{if } a \text{ is a quadric non residue mod } p \end{cases}$$

Example:

$$\begin{aligned} (1/11) &= (4/11) = (9/11) = (5/11) = (3/11) = 1 \\ (2/11) &= (6/11) = (7/11) = (8/11) = (10/11) = -1 \end{aligned}$$

**Theorem.**  $p$  an odd prime,  $p \nmid a$ ,  $p \nmid b$ . Then:

- a)  $a \equiv b[p] \Rightarrow (a/p) = (b/p)$
- b)  $(a^2/p) = 1$
- c)  $(a/p) \equiv a^{\frac{p-1}{2}}[p]$
- d)  $(ab/p) \equiv (a/p)(b/p)$
- e)  $(1/p) = 1 \quad (-1/p) = (-1)^{\frac{p-1}{2}}$

The proofs are quite easy so they will not figure here.

**Corollary:**

$$(-1/p) = \begin{cases} 1 & \\ -1 & \end{cases} \iff \begin{cases} p \equiv 1[4] \\ p \equiv 3[4] \end{cases}$$

*Proof.*

$$p \equiv 1[4] \Rightarrow p = 4k + 1, p \equiv 3[4] \Rightarrow p = 4k + 3$$

$$\text{Since } (-1/p) = (-1)^{\frac{p-1}{2}}, \text{ we have } \begin{cases} (-1)^{2k} = 1 \\ (-1)^{2k+1} = -1 \end{cases}$$

□

$$\text{Example: } (76/43) \stackrel{(a)}{=} (-10/43) \stackrel{(d)}{=} (-1/43)(2/43)(5/43) = (-1) \cdot 1 \cdot 1 = -1$$

**Theorem.** There are infinitely many primes of the form  $4k + 1$

*Proof.* : Assume  $p_1 \dots p_n$  are all the primes  $\equiv 1[4]$ , and set:

$$N = (2p_1p_2 \dots p_n)^2 + 1$$

Let  $p$  be a factor in  $N$ , then  $p$  is odd since  $N$  is odd.

$$\begin{aligned} p \mid N, \quad N &\equiv 0[p] \\ (2p_1p_2 \dots p_n)^2 + 1 &\equiv 0[p] \\ \Rightarrow (2p_1 \dots p_n)^2 &\equiv -1[p] \\ \Rightarrow (-1/p) &= 1 \\ \Rightarrow p &\equiv 1[4] \\ \Rightarrow p \mid N - (2p_1 \dots p_n)^2 &= 1: \text{ absurd!} \end{aligned}$$

Hence there exists infinitely many primes  $\equiv 1[4]$ . □

# Number Theory

November 25

2014

**Gauss's lemma:**  $p$  an odd prime,  $p \nmid a$

Let  $n$  denote the number of elements in

$$S = \{a, 2a, \dots, (\frac{p-1}{2})a\}$$

whose remainders  $[p]$  lie in  $(\frac{p}{2}, p)$ , then:

$$(a/p) = (-1)^n$$

*Proof.* Denote the remainders:  $0 < r_1 < \dots < r_m < \frac{p}{2} < s_1 < \dots < s_n < p$

If we set  $m = |\{r_i\}|$ , and  $n = |\{s_j\}|$ ,  $m + n = \frac{p-1}{2}$

$(r_1, \dots, r_m, p - s_1, \dots, p - s_n)$  are distincts and exhaust  $\{1, 2, \dots, \frac{p-1}{2}\}$ .

Now assume  $p - s_i = r_j$  for some  $i, j$ .

$$\exists n, r \in \mathbb{Z} / 1 \leq u, v \leq \frac{p-1}{2}$$

$$\left. \begin{array}{l} r_j \equiv va[p] \\ s_i \equiv ua[p] \end{array} \right\} \Rightarrow \begin{array}{l} (u+v)a \equiv v_j + s_i = p \equiv 0[p] \\ \Rightarrow p \mid (u+v) \text{ or } p \mid a \text{ (contradiction with the initial conditions)} \\ \Rightarrow p \mid (u+v) \text{ but } 0 < 2 \leq (u+v) \leq p-1 < p \end{array}$$

So  $p \nmid (u+v)$ .

$$\begin{aligned} \left(\frac{p-1}{2}\right)! &= r_1 \dots r_m (p - s_1) \dots (p - s_n) \\ &= r_1 \dots r_m (-s_1) \dots (-s_n) \\ &= (-1)^n r_1 \dots r_m s_1 \dots s_n \\ &= (-1)^n (a(2a) \dots (\frac{p-1}{2})a) \\ &\equiv (-1)^n \left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}} [p] \quad \text{and } \gcd(\frac{p-1}{2}, p) = 1 \text{ so:} \\ 1 &\equiv (-1)^n a^{\frac{p-1}{2}} [p] \\ \Rightarrow (-1)^n &\equiv a^{\frac{p-1}{2}} [p] \end{aligned}$$

And by Euler's criterion:

$$\begin{aligned} (a/p) &\equiv a^{\frac{p-1}{2}} \equiv (-1)^n [p] \\ &\Rightarrow (a/p) \in \{\pm 1\} \end{aligned}$$

Since  $p > 2$ , the congruence must be an equality. □

Example:  $p = 13$ ,  $a = 5$

$$S = \{5, 10, 15, 20, 25, 30\} \equiv \{5, 10, 2, 7, 12, 4\}$$

$$(5/13) = (-1)^5 = -1 \text{ so } 5 \text{ is a non residue [13]}$$

**Definition.**  $\lfloor x \rfloor$  is the largest integer less or equal to  $x$ .

**Theorem.**  $p$  an odd prime, then:

$$(2/p) = \begin{cases} 1 & \text{if } p \equiv \pm 1[8] \\ -1 & \text{if } p \equiv \pm 3[8] \end{cases}$$

*Proof.*  $(2/p) = (-1)^n$ , with  $n$  the number of remainders in  $(\frac{p}{2}, p)$ , from  $S = \{2, 4, 6, \dots, (\frac{p-1}{2})2\}$ .

$p$	$\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor = n$	$(-1)^n = (2/p)$
$8k+1$	$4k - 2k = 2k$	1
$8k+3$	$4k+1 - 2k = 2k+1$	-1
$8k+5$	$4k+2 - (2k+1) = 2k+1$	-1
$8k+7$	$4k+3 - (2k+1) = 2k+2$	1

□

**Corollary:**  $(2/p) = (-1)^{\frac{p^2-1}{8}}$

*Proof.*

- If  $p = 8k \pm 1$   
 $\Rightarrow \frac{p^2-1}{8} = 8k^2 \pm 2$  is even.
- If  $p = 8k \pm 3$   
 $\Rightarrow \frac{p^2-1}{8} = 8k^2 \pm 6 + 1$  is odd.

□

**Theorem.**  $p$  an odd prime.

$$\sum_{a=1}^{p-1} (a/p) = 0$$

i.e. there are exactly  $\frac{p-1}{2}$  quadric residues and  $\frac{p-1}{2}$  quadric non residues  $[p]$ .

*Proof.* Let  $r$  be a primitive root modulo  $p$ , then:

$$\begin{aligned} \{1, 2, \dots, p-1\} &\equiv \{r, r^2, \dots, r^{p-1}\}[p] \\ \sum_{a=1}^{p-1} (a/p) &\underset{\text{Euler's crit}}{=} \sum_{k=1}^{p-1} (r^k/p) = \sum_{k=1}^{p-1} (r/p)^k = \sum_{k=1}^{p-1} (-1)^k \\ (r/p) &\overset{\text{Euler's crit}}{=} r^{\frac{p-1}{2}} \equiv (-1)[p] \\ (r/p) &= -1 \end{aligned}$$

And since  $p-1$  is even, the sum vanishes.

□

# Number Theory

November 28

2014

**Lemma:** Let  $p$  be an odd prime,  $a$  an odd integer,  $p \nmid a$ .

Then,  $(a/p) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor}$

*Proof.* Consider  $S = \{a, 2a, \dots, (\frac{p-1}{2})a\}$ .

$$ka = q_k p + t_k \quad \text{with} \quad 1 \leq t_k \leq p-1, \quad 1 \leq k \leq \frac{p-1}{2}$$

$$\{t_1 \dots t_{\frac{p-1}{2}}\} = \{r_i\}_{i=1}^m + \{s_j\}_{j=1}^n$$

$$\frac{ka}{p} = q_k + \frac{t_k}{p} \quad 0 < \frac{t_k}{p} < 1 \Rightarrow q_k = \lfloor \frac{ka}{p} \rfloor$$

The we calculate the two sums:

•

$$\sum_{k=1}^{\frac{p-1}{2}} ka = \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor + \sum_{i=1}^m r_i + \sum_{j=1}^n s_i$$

• And considering  $\{r_i, p - s_j\} = \{t_1, t_2, \dots, \frac{p-1}{2}\}$  (from a previous result),

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{i=1}^m r_i + \sum_{j=1}^n (p - s_j) = np + \sum r_i + \sum s_j$$

We then subtract:

$$\sum_{k=1}^{\frac{p-1}{2}} ak - \sum_{k=1}^{\frac{p-1}{2}} k = p \left( \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor - n \right) + 2 \sum s_j$$

And looking at that modulo 2, with  $a$  and  $p$  both still odd:

$$0 \equiv \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor - n[2]$$

$$\Rightarrow \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor \equiv n[2] \quad \text{but then} \quad (a/p) = (-1)^n = (-1)^{\sum \lfloor \frac{ka}{p} \rfloor}$$

□

**Gauss's quadratic reciprocity theorem:**

$p \neq q$  two odd primes, then:

$$(p/q)(q/p) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$$

The exact proof is in the book. **Corollary:**  $p \neq q$  two odd primes, then

$$(p/q)(q/p) = \begin{cases} 1 & \text{if } p \text{ or } q \equiv 1[4] \\ -1 & \text{if } p \text{ or } q \equiv 3[4] \end{cases}$$

**Corollary:**  $p \neq q$  two odd primes, then

$$(p/q) = \begin{cases} (q/p) & \text{if } p \text{ or } q \equiv 1[4] \\ -(q/p) & \text{if } p \text{ or } q \equiv 3[4] \end{cases}$$

Example:

$$(37/89) \Rightarrow \left. \begin{array}{l} 37 \equiv 1[4] \\ 89 \equiv 15[37] \end{array} \right\} \Rightarrow (15/37) = (3/37)(5/37) = (1/3)(2/5) = 1 \cdot -1 = -1$$

**Theorem.** *If  $p \neq 3$  is an odd prime, then*

$$(3/p) = \begin{cases} 1 & \text{if } p \equiv \pm 1[12] \\ -1 & \text{if } p \equiv \pm 5[12] \end{cases}$$



# Number Theory

December 2

2014

Question: What integer can be written as a sum of 2 squares?

**Lemma:**

$$\text{If } \begin{cases} m = a^2 + b^2 \\ n = c^2 + d^2 \end{cases} \Rightarrow mn \text{ is also a sum of two squares.}$$

*Proof.*

$$\begin{aligned} \text{Set } \begin{cases} z = a + bi \\ w = c + di \end{cases} & \begin{cases} m = a^2 + b^2 = |z|^2 \\ n = c^2 + d^2 = |w|^2 \end{cases} \\ (a^2 + b^2)(c^2 + d^2) = mn &= |z|^2 |w|^2 = |zw|^2 \\ &= |(a + bi)(c + di)|^2 \\ &= |(ac - bd) + (ad + bc)i| \\ &= (ac - bd)^2 + (ad + bc)^2 \end{aligned}$$

□

**Dirichlet's box principle:** If  $n$  objects are placed in  $m$  boxes, and  $n > m$ , then some boxes contains more than one object.

Thue's Lemma:  $p$  a prime,  $a \in \mathbb{Z}$ ,  $p \nmid a$

Then  $ax \equiv y[p]$  has a solution  $x_0, y_0 \in \mathbb{Z}/$

$$0 < |x_0| < \sqrt{p}, \quad 0 < |y_0| < \sqrt{p}$$

*Proof.* Set  $k = \lfloor \sqrt{p} \rfloor + 1$ , and consider:

$$\begin{aligned} f : \{0, 1, \dots, k-1\} \times \{0, 1, \dots, k-1\} &\longrightarrow \{0, 1, \dots, q-1\} \\ (x, y) &\longrightarrow ax - y[p] \end{aligned}$$

As  $k > p^2$ , Dirichlet's box principle implies:  $\exists (x_1, y_1) \neq (x_2, y_2) /$

$$\begin{aligned} f(x_1, y_1) &= f(x_2, y_2) \\ ax_1 - y_1 &= ax_2 - y_2[p] \\ ax_1 - ax_2 &= y_1 - y_2[p] \\ \begin{pmatrix} x_0 = x_1 - x_2 \\ y_0 = y_1 - y_2 \end{pmatrix} &\rightarrow ax_0 = y_0[p] \end{aligned}$$

We prove easily that  $x_0$  and  $y_0$  are both non zero.

□

**Fermat's theorem:** An odd prime  $p$  is a sum of 2 squares iff  $p \equiv 1[4]$ .

*Proof.* :

$\Rightarrow$  Assume

$$p = a^2 + b^2 \quad a, b \in \mathbb{N}$$

Then  $p \nmid a$ , for if it does:

$$a = pk \implies p = a^2 + b^2 \geq a^2 = p^2 k \geq p^2$$

Symetrically,  $p \nmid b$ .

Then,  $\exists c \in \mathbb{Z}/p\mathbb{Z} \quad bc \equiv 1[p]$ , and:

$$\begin{aligned} c^2 \mid (ac)^2 + (bc)^2 &= (a^2 + b^2)c^2 = pc^2 \equiv 0[p] \\ \Rightarrow (ac)^2 + 1 &\equiv 0[p] \\ ac^2 &\equiv -1[p] \\ (-1/p) &= 1 \Rightarrow p \equiv 1[4] \end{aligned}$$

$\Leftarrow$  Let  $p \equiv 1[4]$

$$\Rightarrow (-1/p) = 1$$

$$\Rightarrow a^2 \equiv -1[p]$$

Then  $a \not\equiv 0[p]$  so  $p \nmid a$  and Thue's lemma says  $\exists x, y \in \mathbb{Z}/p\mathbb{Z}$

$$ax \equiv y[p]$$

$$0 < |x| < \sqrt{p}, \quad 0 < |y| < \sqrt{p}$$

$$y^2 \equiv (ax)^2 = a^2 x^2 \equiv -x^2[p]$$

$$\Rightarrow x^2 + y^2 \equiv 0[p]$$

$$x^2 + y^2 = kp \quad \text{for some } p \in \mathbb{Z}$$

$$0 < x^2 + y^2 < p + p = 2p$$

$$\Rightarrow k = 1, \quad x^2 + y^2 = p$$

□

**Proposition:**  $p$  a prime of the form  $4k + 1$  can be represented uniquely as a sum of two squares.

*Proof.* Assume  $p = a^2 + b^2 = c^2 + d^2$  where  $a, b, c, d$  are positive integers.

Then

$$\begin{aligned} a^2 d^2 - b^2 d^2 &= a^2 d^2 + b^2 d^2 - b^2 d^2 - b^2 c^2 \\ &= d^2(a^2 + b^2) - b^2(c^2 + d^2) \\ &= d^2 p - b^2 p \equiv 0[p] \end{aligned}$$

So  $p \mid (ad + bc)$  or  $p \mid (ad - bc)$ . Now

$$\begin{aligned} 0 < a, b, c, d < \sqrt{p} &\Rightarrow 0 < ad, bc < p \\ \Rightarrow ad = bc &\quad \text{or} \quad ad = p - bc \end{aligned}$$

In this last case,  $p = ad + bc$ , so:

$$\begin{aligned} p^2 &= (a^2 + b^2)(a^2 + d^2) = (ad + bc)^2 + (ac - bd)^2 = p^2 + (ac - bd)^2 \\ &\Rightarrow ac - bd = 0 \\ &\quad ac = bd \end{aligned}$$

Then we have either  $ad = bc$  or  $ac = bd$ .

By symmetry ( $c \rightarrow d$ ) we assume  $ad = bc$ .

If  $\gcd(a, b) > 1$ , then

$$\gcd(a, b)^2 \mid a^2 + b^2 = p^2$$

Which is absurd, therefore,  $a$  and  $b$  are relatively prime.

$$\begin{aligned} a \mid ad = bc &\Rightarrow a \mid c \\ c &= ka, \quad \text{for some } k \in \mathbb{Z} \end{aligned}$$

$$\begin{aligned} ad &= bka \\ d &= bk \\ (c, d) &= k(a, b) \\ p &= c^2 + d^2 = (ka)^2 + (kb)^2 = k^2(a^2 + b^2) = k^2p \\ &\Rightarrow k^2 = 1 \\ &\Rightarrow k = 1 \\ &\Rightarrow (c, d) = (a, b) \end{aligned}$$

□

Example:  $p = 29 \equiv 1[4]; a^2 \equiv -1[29]$

$$a = 12; \quad 12^2 = 144 \equiv -1[29]$$

$$12x \equiv y[29] \quad 145 = 5 \cdot 29$$

$$0 < |x|, |y| < \sqrt{29}$$

$x$	$12x \equiv y$
1	$12 \equiv 12$
2	$24 \equiv -5$
3	$36 \equiv 7$
4	$48 \equiv -10$
5	$50 \equiv 2$

$$\begin{aligned} (x, y) &= (2, -5) \\ 12 \cdot 2 &\equiv -5[29] \\ 5^2 = y^2 &\equiv (12x)^2 \equiv -1x^2 \equiv -2^2[29] \\ 5^2 + 2^2 &\equiv 0[29] \\ 5^2 + 2^2 &= 29 \end{aligned}$$

**Theorem.** Let  $n \in \mathbb{N}$ ,  $n = N^2m$ , with  $m$  square free.  
Then  $n = a^2 + b^2 \iff m$  contains no prime factor of the form  $4k + 3$

*Proof.* :

$\Rightarrow$  Assume

$$n = a^2 + b^2 = N^2 m$$

Let  $p$  be an odd prime,  $p \mid m$ . Set:

$$\begin{aligned} d &= \gcd(a, b) \\ a &= dr \\ b &= ds \end{aligned} \quad \text{with } \gcd(r, s) = 1$$

$$d^2(r^2 + s^2) = (dr)^2 + (ds)^2 = a^2 + b^2 = n = N^2 m$$

$$\Rightarrow d^2 \mid N^2 \text{ as } m \text{ is square free?}$$

$$r^2 + s^2 \equiv 0[p]$$

$$\gcd(r, s) = 1 \equiv p \nmid r \text{ or } p \nmid s$$

By symmetry,  $p \nmid r$ .

$\exists r' \in \mathbb{Z}/$

$$\begin{aligned} rr' &\equiv 1[p] \\ (rr')^2 + (sr')^2 &\equiv 0[p] \\ 1 + (sr')^2 &\equiv 0[p] \\ (sr')^2 &\equiv -1[p] \\ \Rightarrow (-1/p) &= 1 \\ \Rightarrow p &\equiv 1[4] \end{aligned}$$

$\Leftarrow$  If  $m = 1$ ,  $n = N^2$ .

Let  $m > 1$ ,  $m = p_1 \dots p_r$  (distinct primes).  $p_i \equiv 1 \text{ or } 2[4]$ ,  $\exists x_i, y_i \in \mathbb{Z}/$

$$p_i = x_i^2 + y_i^2 \quad 1 \leq i \leq r$$

By repeatedly using multiplicativity:

$$\begin{aligned} m &= p_1 \dots p_r = x^2 + y^2 \\ n &= N^2 m = N^2(x^2 + y^2) = (Nx)^2 + (Ny)^2 = a^2 + b^2 \end{aligned}$$

□

Example:

•

$$459 = 3^3 \cdot 17 = \underbrace{3^2}_{N^2} \underbrace{(3 \cdot 17)}_m$$

$$3 = 3[4] \text{ so } n = 459 \neq a^2 + b^2.$$

•

$$n = 153 = 3^2 \cdot 17$$

$$m = 4^2 + 1^2$$

$$153 = 3^2(4^2 + 1^2) = (3 \cdot 4)^2 + 3^2 = 12^2 + 3^2$$

**Theorem.** «Officially part of the course but not so important»  $n \in \mathbb{Z}$  can be written  $n = a^2 + b^2 \iff n \not\equiv 2[4]$

# Number Theory

December 5

2014

## Fibonacci sequence

$$\begin{cases} u_1 = u_2 = 1 \\ u_n = u_{n-1} + u_{n-2} \end{cases}$$

Claim:  $u_{5n+2} > 10^n$  for  $n \geq 1$ .

*Proof.* Induction on  $n$ :

$$n = 1 \quad u_7 = 13 > 10^1$$

Now assume it is true for some  $n$ :

$$\begin{aligned} u_{5n+2} &> 10^n \\ u_{5(n+1)+2} &= u_{5n+7} = u_{5n+6} + u_{5n+5} \\ &= 2(u_{5n+5} + u_{5n+3}) + u_{5n+4} \\ &= 3(u_{5n+3} + u_{5n+2}) + 2u_{5n+3} \\ &= 5(u_{5n+2} + u_{5n+1}) + 3u_{5n+2} \\ &= 8u_{5n+2} + 5u_{5n+1} > 8u_{5n+2} + 2 \underbrace{(u_{5n+1} + u_{5n})}_{=u_{5n+2}} \\ &= 10u_{5n+2} > 10 \cdot 10^n = 10^{n+1} \end{aligned}$$

□

**Theorem.**  $\gcd(u_n, u_{n+1}) = 1 \quad \forall n \geq 1$

*Proof.* Set  $d = \gcd(u_n, u_{n+1})$

$$\begin{aligned} &\Rightarrow d \mid u_{n+1} - u_n = u_{n-1} \\ &\Rightarrow d \mid u_n - u_{n-1} = u_{n-2} \\ &\Rightarrow \vdots \\ &\Rightarrow d \mid u_3 - u_2 = 1 \\ &\Rightarrow d = 1 \end{aligned}$$

□

Proposition: for  $m \geq 2, n \geq 1$ :

$$u_{m+n} = u_{m-1}u_n + u_mu_{n+1}$$

*Proof.* Fix  $m \geq 2$ . Induction on  $n$ :

$$\boxed{n=1} \quad \begin{aligned} u_{m+1} &= u_{m-1}u_1 + u_mu_2 \\ &= u_{m-1} + u_m \end{aligned}$$

Now assume it is true for all integer until some  $n$ . We show it is true for  $n + 1$ :

$$\begin{aligned}
\text{at } n-1 \quad u_{m+n-1} &= u_{m-1}u_{n-1} + u_mu_n \\
\text{at } n \quad u_{m+n} &= u_{m-1}u_n + u_mu_{n+1} \\
\text{at } n+1 \quad u_{m+n+1} &= u_{m-1}u_{n-1} + u_mu_n + u_{m-1}u_n + u_mu_{n+1} \\
&= u_{m-1}(u_n + u_{n-1}) + u_m(u_n + u_{n+1}) \\
&= u_mu_{n+1} + u_mu_{k+2}
\end{aligned}$$

□

**Theorem.** For  $m \geq 1, n \geq 1$

$$u_m \mid u_{mn}$$

*Proof.* Fix  $m \geq 1$  and by induction on  $n$ :

$$\boxed{n=1} \quad u_m \mid u_{m \cdot 1} = u_m$$

Now assume  $u_m \mid u_{mn}$  for some  $n$ , and consider the case  $n + 1$ :

$$\begin{aligned}
u_{m(n+1)} &= u_{mn+n} = u_{mn-1}u_m + u_{mn}u_{m+1} \\
\Rightarrow u_m \mid u_m; \quad u_m \mid u_{mn} &\Rightarrow u_m \mid u_{mn-1}u_m + u_{mn}u_{m+1} \\
&\Rightarrow u_m \mid u_{m(n+1)}
\end{aligned}$$

□

**Lemma:** Let  $m = qn + r$ , with  $m, n, q, r \geq 1$ , then:

$$\gcd(u_m, u_n) = \gcd(u_r, u_n)$$

*Proof.*

$$\begin{aligned}
\gcd(u_m, u_n) &= \gcd(u_{qn+r}, u_n) \\
&= \gcd(u_{qn-1}u_r + u_{qn}u_{r+1}, u_n)
\end{aligned}$$

$$\begin{aligned}
[\text{We know that: } u_n \mid u_{qn} \Rightarrow \gcd(a + bk, b) &= \gcd(a, b)] \\
&= \gcd(u_{qn-1}u_r, u_n)
\end{aligned}$$

We now try to prove:

$$\gcd(u_{qn-1}, u_n) = 1$$

$$\text{If } d = \gcd(u_{qn-1}, u_n) \text{ then } d \mid u_n \mid u_{qn} \Rightarrow \begin{cases} d \mid u_{qn-1} \\ d \mid u_{qn} \end{cases} \Rightarrow d = 1$$

□

**Theorem.** The gcd of two Fibonacci numbers is a Fibonacci number:

$$\gcd(u_m, u_n) = u_{\gcd(m, n)}$$

*Proof.* Assume  $m \geq n$ . We use the euclidian algorithm:

$$\begin{array}{ll|l}
m = q_1n + r_1 & 0 < r_1 < n & \gcd(u_m, u_n) = \gcd(u_{r_1}, u_n) \\
n = q_2r_1 + r_2 & 0 < r_2 < r_1 & = \gcd(u_n, u_{r_1}) = \gcd(u_{r_2}, u_{r_1}) \\
\vdots & \vdots & = \cdots = \gcd(u_{r_{k-1}}, u_{r_k}) \\
r_{k-2} = q_k r_{k-1} + r_k & & \text{And since } r_k \mid r_{k-1} \Rightarrow u_{r_k} \mid u_{r_{k-1}} \\
r_{k-1} = q_{k-1} r_k + 0 & 0 < r_k < r_{k-1} & \text{We have } u_{\gcd(m, n)}
\end{array}$$

□

# Number Theory

December 9

2014

**Definition.** A finite continued fraction is an expression:

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_{n-1} + \frac{1}{a_n}}}}}$$

**Theorem.** Any rational number can be written as a finite simple continued fraction.

*Proof.* in the book p.308. □

Example:

$$\begin{array}{l|l} \frac{a}{b} = \frac{43}{13} & \frac{43}{13} = 3 + \frac{4}{13} = 3 + \frac{1}{\frac{13}{4}} \\ 43 = 3 \cdot 13 + 4 & \frac{13}{4} = 3 + \frac{1}{4} = 3 + \frac{1}{4} \cdot 1 \\ 13 = 3 \cdot 4 + 1 & \frac{4}{1} = 4 \\ 4 = 4 \cdot 1 & \end{array}$$

$$\Rightarrow \frac{43}{13} = 3 + \frac{1}{3 + \frac{1}{4}}$$

$$\Rightarrow \frac{13}{43} = 0 + \frac{1}{3 + \frac{1}{3 + \frac{1}{4}}}$$

Notation:  $[a_0; a_1, a_2, \dots, a_n] = a_0 + \frac{1}{a_1 + \frac{1}{\ddots + \frac{1}{a_{n-1} + \frac{1}{a_n}}}}$

$$\frac{13}{43} = [0; 3, 3, 4]$$

**Definition.**  $C_k = [a_0; a_1, a_2, \dots, a_k]_{1 \leq k \leq n}$ ; is called the  $k^{th}$  convergent to  $[a_0; a_1, \dots, a_k, \dots, a_n]$ .

Example:

$$\left. \begin{array}{l} [0; 3, 3, 4] \\ C_0 = 0 \\ C_1 = 0 + \frac{1}{3} = \frac{1}{3} \\ C_2 = 0 + \frac{1}{3 + \frac{1}{3}} = \frac{3}{10} \\ C_3 = 0 + \frac{1}{3 + \frac{1}{3 + \frac{1}{4}}} = \frac{13}{43} \end{array} \right\} C_k = \frac{p_k}{q_k}, \text{ with } \begin{bmatrix} p_0 = a_0 & q_0 = 1 \\ p_1 = a_1 a_0 + 1 & q_1 = a_1 \\ p_k = a_k p_{k-1} & q_k = a_k q_{k-1} + q_{k-2} \end{bmatrix}$$

**Theorem.** The  $k^{th}$  convergent  $C_k = \frac{p_k}{q_k}$  with  $p_k, q_k$  given by recursion.

*Proof.* We prove this more generally for  $a_0, a_1, \dots, a_n \in \mathbb{R}$ .

Induction on  $k$ : True for  $C_0 = \frac{p_0}{q_0}$ ,  $C_1 = \frac{p_1}{q_1}$ ,  $C_2 = \frac{p_2}{q_2}$ .

Now assume it's true for some  $m$  such that:  $2 \leq m \leq n$ :

$$[a_0; a_1, \dots, a_m] = \frac{p_m}{q_m} = \frac{a_m p_{m-1} + p_{m-2}}{a_m q_{m-1} + q_{m-2}}$$

Since  $p_{m-1}, p_{m-2}, q_{m-1}, q_{m-2}$  only depend on  $a_0, a_1, \dots, a_{m-1}$  but not  $a_m$ :

$$\begin{aligned} C_{m+1} &= [a_0; a_1, \dots, a_m, a_{m+1}] = [a_0; a_1, \dots, a_m + \frac{1}{a_{m+1}}] \\ &= \frac{(a_m + \frac{1}{a_{m+1}})p_{m-1} + p_{m-2}}{(a_m + \frac{1}{a_{m+1}})q_{m-1} + q_{m-2}} \cdot \frac{a_{m-1}}{a_{m-1}} \\ &= \frac{a_{m+1}(a_m p_{m-1} + p_{m-2}) + p_{m-1}}{a_{m+1}(a_m q_{m-1} + q_{m-2}) + q_{m-1}} \\ &= \frac{p_{m+1}}{q_{m+1}} \end{aligned}$$

Therefore, the theorem holds for  $m+1$  and for all  $m \leq n$  by finite induction.  $\square$

Convention:

$$\left\{ \begin{array}{ll} p_{-2} = 0 & q_{-2} = 1 \\ p_{-1} = 1 & q_{-1} = 0 \end{array} \right. \quad \left( \begin{array}{c|c|c|c|c|c|c} k & -2 & -1 & 0 & 1 & 2 & 3 \\ \hline a_k & . & . & 0 & 3 & 3 & 4 \\ p_k & 0 & 1 & 0 & 1 & 3 & 13 \\ q_k & 1 & 0 & 1 & 3 & 10 & 43 \\ C_k & . & . & 0 & \frac{1}{3} & \frac{3}{10} & \frac{13}{43} \end{array} \right)$$

**Theorem.** The convergents  $\frac{p_k}{q_k} \quad \forall k \leq n$  satisfy:

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$$

*Proof.*

$$\begin{bmatrix} p_k & q_k \\ p_{k-1} & q_{k-1} \end{bmatrix} = \begin{bmatrix} a_k & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} p_{k-1} & q_{k-1} \\ p_{k-2} & q_{k-2} \end{bmatrix}$$

If we set  $M_k = \begin{bmatrix} p_k & q_k \\ p_{k-1} & q_{k-1} \end{bmatrix}$ ; and  $A_k = \begin{bmatrix} a_k & 1 \\ 1 & 0 \end{bmatrix}$ , then:  $M_k = A_k M_{k-1}$ . And therefore:

$$A_k M_{k-1} = A_k (A_{k-1} M_{k-2}) = \dots = A_k A_{k-1} \dots A_0 M_{-1}$$

$$M_{-1} = \begin{bmatrix} p_{-1} & q_{-1} \\ p_{-2} & q_{-2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = Id$$

$$\begin{aligned} \Rightarrow \det(M_k) &= p_k q_{k-1} - q_k p_{k-1} = \prod_{j=0}^k \det(A_j) \det(M_{-1}) = (-1)^{k+1} \\ &= (-1)^{k-1} \end{aligned}$$

$\square$



# Number Theory

December 9

2014

**Lemma:**  $q_{k-1} \leq q_k$  for  $A \leq k \leq n$  with a strict inequality for  $k > 1$ .  
Hence  $q_k \rightarrow \infty$  as  $k \rightarrow \infty$ .

*Proof.* :  $k = 1$ ,  $q_k = 1 \leq a_1 = q_1$ , and let  $k > 1$ , then:

$$q_k = a_k q_{k-1} + q_{k-2} > a_k q_{k-1} \geq q_{k-1}$$

□

**Theorem.** *The convergents satisfy:*

- a)  $C_0 < C_2 < C_4 < \dots$
- b)  $C_1 < C_3 < C_5 < \dots$
- c)  $C_{2s} < C_{2r-1} \quad \forall s \geq 0, r \geq 1$ .

*Proof.*

$$\begin{aligned} C_{k+2} - C_k &= (C_{k+2} - C_{k+1}) + (C_{k+1} - C_k) \\ &= \left( \frac{p_{k+2}}{q_{k+2}} - \frac{p_{k+1}}{q_{k+1}} \right) + \left( \frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k} \right) \\ &= \frac{(-1)^{k+1}}{q_{k+2}q_{k+1}} + \frac{(-1)^k}{q_{k+1}q_k} = (-1)^k \frac{q_{k+2} - q_k}{q_{k+2}q_{k+1}q_k} \\ &\Rightarrow \begin{cases} \text{If } k \text{ is even : } C_{k+2} - C_k > 0 \Rightarrow C_k < C_{k+2} & (a) \\ \text{If } k \text{ is odd : } C_{k+2} - C_k < 0 \Rightarrow C_{k+2} < C_k & (b) \end{cases} \end{aligned}$$

□

**Definition.** *An infinite continued fraction is an expression:*

$$[a_0; a_1, a_2, \dots, a_n, \dots] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\ddots}}}}$$

With  $a_j \in \mathbb{Z}$   $a_j > 0$  for  $j \geq 1$

This has a convergent  $C_n$ :

$$C_n = [a_0; a_1, a_2, \dots, a_n] = \lim_{n \rightarrow \infty} C_n$$

Proof of the convergence:

$$C_0 < C_2 < C_4 < \dots < C_5 < C_3 < C_1$$

Set

$$\left. \begin{aligned} \alpha &= \lim_{n \rightarrow \infty} C_{2n} \\ \alpha' &= \lim_{n \rightarrow \infty} C_{2n-1} \end{aligned} \right\} \alpha \leq \alpha'$$

$$0 \leq \alpha - \alpha' < C_{2n+1} - C_{2n} = \frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} = \frac{(-1)^{2n}}{q_{2n+1}q_{2n}} = \frac{1}{\underbrace{q_{2n+1}q_{2n}}_{\rightarrow 0 \text{ when } n \rightarrow \infty}}$$

Example: Consider  $[1; 1, 1, 1, \dots, 1, \dots]$   $a_n = 1 \forall n$ .

$$p_n = p_{n-1} + p_{n-2} \quad q_n = q_{n-1} + q_{n-2}$$

$k$	-2	-1	0	1	2	3	4	5
$p_k$	0	1	1	2	3	5	8	13
$q_k$	1	0	11	2	3	5	8	

$$\Rightarrow C_n = \frac{u_{n+2}}{u_{n+1}} \text{ since it's the Fibonnacci sequence.}$$

$$\Rightarrow \lim_{n \rightarrow \infty} C_n = \lim_{n \rightarrow \infty} \frac{u_{n+2}}{u_{n+1}} = \lim_{n \rightarrow \infty} \frac{u_{n+2}}{u_{n+1}} = \lim_{n \rightarrow \infty} \frac{u_{n+1} + u_n}{u_{n+1}} = \lim_{n \rightarrow \infty} 1 + \frac{1}{\frac{u_{n+1}}{u_n}} = \lim_{n \rightarrow \infty} 1 + \frac{1}{\lim_{n \rightarrow \infty} \frac{u_{n+1}}{u_n}}$$

$$\Rightarrow \lim_{n \rightarrow \infty} \frac{u_{n+2}}{u_{n+1}} = \frac{\lim_{n \rightarrow \infty} \frac{u_{n+2}}{u_{n+1}} + 1}{\lim_{n \rightarrow \infty} \frac{u_{n+2}}{u_{n+1}}} \Rightarrow \lim_{n \rightarrow \infty} C_n = \frac{\lim_{n \rightarrow \infty} C_n + 1}{\lim_{n \rightarrow \infty} C_n} \Rightarrow (\lim_{n \rightarrow \infty} C_n)^2 = \lim_{n \rightarrow \infty} C_n + 1$$

$$\Rightarrow x^2 - x + 1 = 0 \iff x = \frac{1 \pm \sqrt{5}}{2} \text{ but } x_0 > C_0 \Rightarrow \frac{1 + \sqrt{5}}{2}$$

$$\Rightarrow \frac{1 + \sqrt{5}}{2} = [1; 1, 1, \dots]$$

Notation: We write:

$$[3; 1, 2, 1, 6, 1, 2, 1, 6, 1, \dots] = [3; 1, 2, \bar{1}, 6]$$

**Theorem.** *The value of an infinite continued fraction is irrational.*

*Proof.* Set  $x = [a_0, a_1, \dots, a_n, \dots] = \lim_{n \rightarrow \infty} C_n = \lim_{n \rightarrow \infty} \frac{p_n}{q_n}$

Let  $n \geq 0$ . As  $x$  lies between  $C_n$  and  $C_{n+1}$

$$0 < |x - C_n| < |C_{n+1} - C_n| = \left| \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \right| = \frac{1}{q_{n+1}q_n}$$

Now, assume (for a contradiction) that  $x = \frac{a}{b} \in \mathbb{Q}$ :

$$0 < \left| \frac{a}{b} - \frac{p_n}{q_n} \right| < \frac{1}{q_{n+1}q_n}$$

□