8. Primitive Roots

We recall the Euclidean algorithm: for $a,b \in \mathbb{Z}$, there exist $x,y \in \mathbb{Z}$ such that $ax+by = (a,b)$.

Theorem 41 (Chinese Remainder Theorem): Let $m_1,\dots,m_t \in \mathbb{Z}$ with $(m_i,m_j)=1$ for $i \neq j$, and let $m = m_1 \cdots m_t$. Let $b_1,\dots,b_t \in \mathbb{Z}$. Then the simultaneous congruences

$$x \equiv b_1 \pmod{m_1}$$

$$x \equiv b_t \pmod{m_t}$$

has a unique solution modulo m.

Proof: Let $n_i = \frac{m}{m_i}$ $(1 \leq i \leq t)$. Then $(m_i,n_i)=1$. Then there exist $r_i,s_i \in \mathbb{Z}$ such that $r_i n_i + s_i m_i = 1$ $(1 \leq i \leq t)$. Let $e_i = r_i n_i$. Then $e_i \equiv 1 \pmod{m_i}$ and $e_i \equiv 0 \pmod{m_j}$ for $i \neq j$. Consider

$$x_0 = \sum_{i=1}^{t} b_i e_i.$$

Then $x_0 \equiv b_i \pmod{m_i}$ $(1 \leq i \leq t)$, i.e. it is a solution of the simultaneous congruences. To prove the uniqueness of x_0, suppose $x_1 \equiv b_i \pmod{m_i}$ $(1 \leq i \leq t)$. Then $m_i \mid (x_1 - x_0)$ $(1 \leq i \leq t)$. Since $(m_i,m_j)=1$ for $i \neq j$ and $m = \prod_{i=1}^{t} m_i$, we have $m \mid (x_1 - x_0)$, i.e. $x_1 \equiv x_0 \pmod{m}$. ∎

For $n \in \mathbb{Z}$, let $(\mathbb{Z}/n\mathbb{Z})^*$ denote the invertible elements in $\mathbb{Z}/n\mathbb{Z}$, i.e. they are the congruence classes $r+n\mathbb{Z}$ for which there exists $s+n\mathbb{Z}$ with $(r+n\mathbb{Z})(s+n\mathbb{Z}) = 1+n\mathbb{Z}$. This is equivalent to saying that $(r,n)=1$.

Theorem 42: Let $m_1,\dots,m_t \in \mathbb{N}$ with $(m_i,m_j)=1$ for $i \neq j$, and let $m = m_1 \cdots m_t$. Then

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_t\mathbb{Z}$$

as a ring isomorphism. Also,

$$(\mathbb{Z}/m\mathbb{Z})^* \cong (\mathbb{Z}/m_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/m_t\mathbb{Z})^*$$
as a group isomorphism.

Proof: Let $\psi: \mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_t\mathbb{Z}$ be defined by
$$\psi(n) = (n+m_1\mathbb{Z}, \ldots, n+m_t\mathbb{Z}).$$
One can check that ψ is a ring homomorphism. By the Chinese Remainder Theorem, ψ is surjective and $\ker(\psi) = m\mathbb{Z}$. Thus by the first isomorphism theorem for rings,
$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_t\mathbb{Z}.$$
Let $\lambda: (\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/m_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/m_t\mathbb{Z})^*$ be defined by
$$\lambda(r+m\mathbb{Z}) = (r+m_1\mathbb{Z}, \ldots, r+m_t\mathbb{Z}).$$
Note that $(r,m)=1$ if and only if $(r,m_i)=1$ $(1 \le i \le t)$. Thus the map is well-defined. One can show that λ is a group homomorphism. It is bijective by the Chinese Remainder Theorem. ∎

Corollary 43: Let $m_1, \ldots, m_t \in \mathbb{N}$ with $(m_i, m_j) = 1$ for $i \neq j$, and let $m = m_1 \cdots m_t$. Then
$$\varphi(m) = \varphi(m_1) \cdots \varphi(m_t).$$

Proof: Note that $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|$ and
$$\begin{aligned}\varphi(m_1) \cdots \varphi(m_t) &= |(\mathbb{Z}/m_1\mathbb{Z})^*| \cdots |(\mathbb{Z}/m_t\mathbb{Z})^*| \\ &= |(\mathbb{Z}/m_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/m_t\mathbb{Z})^*|.\end{aligned}$$
Then the result follows from theorem 42. ∎

Corollary 44: Let $m = p_1^{a_1} \cdots p_t^{a_t}$ where $p_1, \ldots, p_t$ are distinct primes and $a_1, \ldots, a_t \in \mathbb{N}$. Then
$$\varphi(m) = m \prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right).$$

Proof: Take $m_i = p_i^{a_i}$ $(1 \le i \le t)$ in corollary 43. Note that
$$\varphi(p_i^{a_i}) = p_i^{a_i} - p_i^{a_i - 1} = p_i^{a_i}\left(1 - \frac{1}{p_i}\right).$$
It follows that
$$\begin{aligned}\varphi(m) &= \varphi(p_1^{a_1}) \cdots \varphi(p_t^{a_t}) \\ &= p_1^{a_1} \cdots p_t^{a_t}\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_t}\right) = m \prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right).\end{aligned}$$
∎

Proposition 45: Let p be a prime. If $d \mid (p-1)$, then $x^d \equiv 1 \pmod p$ has exactly d solutions mod p.

Proof: Write $p-1 = dk$ with $k \in \mathbb{Z}$. Then

$$\frac{x^{p-1}-1}{x^d-1} = \frac{(x^d)^k - 1}{x^d - 1} = (x^d)^{k-1} + \cdots + 1 =: g(x) \in (\mathbb{Z}/p\mathbb{Z})[x].$$

By Fermat's Little Theorem, $x^{p-1}-1$ has $p-1$ distinct roots in $\mathbb{Z}/p\mathbb{Z}$. Thus $(x^d-1)g(x)$ factors into linear factors in $(\mathbb{Z}/p\mathbb{Z})[x]$ and the result follows. ∎

Theorem 46: If p is prime then $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group.

Proof: For each divisor d of $p-1$, let $\lambda(d)$ denote the number of elements of $(\mathbb{Z}/p\mathbb{Z})^*$ of order d. By proposition 45, there are exactly d elements of $(\mathbb{Z}/p\mathbb{Z})^*$ whose order divides d. Thus

$$d = \sum_{c \mid d} \lambda(c).$$

By the Möbius inversion formula,

$$\lambda(d) = \sum_{c \mid d} \mu(c) \frac{d}{c} = d \sum_{c \mid d} \frac{\mu(c)}{c} = d \prod_{p \mid d} \left(1 - \frac{1}{p}\right) = \varphi(d).$$

Thus there are $\varphi(p-1)$ elements of $(\mathbb{Z}/p\mathbb{Z})^*$ of order $p-1$. In particular, $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic. ∎

Remark: For a general $n \in \mathbb{N}$, $(\mathbb{Z}/n\mathbb{Z})^*$ is not always cyclic. For example,

$$(\mathbb{Z}/8\mathbb{Z})^* = \{1+8\mathbb{Z}, 3+8\mathbb{Z}, 5+8\mathbb{Z}, 7+8\mathbb{Z}\}$$

and $1^2 \equiv 1, 3^2 \equiv 1, 5^2 \equiv 1, 7^2 \equiv 1 \pmod 8$. Thus this group is not cyclic.

Def) Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. We say a is a primitive root modulo n if $a + n\mathbb{Z}$ generates $(\mathbb{Z}/n\mathbb{Z})^*$.

2015 11 04

Ex. 2 is a primitive root mod 5 but 2 is not a primitive root mod 7.

Remark: We have seen in the proof of theorem 46 that for a

prime p, $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic. Thus, there exists a primitive root mod p. In fact, we see from the proof that there are $\varphi(p-1)$ primitive root modulo p.
Note that if $a \in \mathbb{N}$ is a square, then it is a quadratic residue mod p. Thus a is not a primitive root mod p.

Artin's Primitive Root Conjecture: If $a \in \mathbb{N}$ is not a perfect square, then a is a primitive root mod p for infinitely many primes p.

The conjecture remains open. In 1967, Hooley proved that the conjecture is true under the assumption of the generalized Riemann hypothesis. In 1980's, using sieve method, Gupta, K. Murty, R. Murty, and Heath-Brown showed unconditionally that given any non-square $a, b, c \in \mathbb{N}$, then at least one of them is a primitive root mod p for infinitely many primes p. For example, one of $2, 3, 5$ is a primitive root mod p for infinitely many primes p. However, the result is not constructive, and thus we do not know which one satisfies the condition.

Proposition 47: Let p be a prime and $\ell \in \mathbb{N}$. If $a \equiv b \pmod{p^\ell}$ then $a^p \equiv b^p \pmod{p^{\ell+1}}$.

Proof: Write $a = b + cp^\ell$ for some $c \in \mathbb{Z}$. Then

$$\begin{aligned} a^p &= (b + cp^\ell)^p \\ &= b^p + \binom{p}{1} b^{p-1} cp^\ell + \binom{p}{2} b^{p-2} (cp^\ell)^2 + \cdots + \binom{p}{p} (cp^\ell)^p \end{aligned}$$

Since $p^{\ell+1} \mid \binom{p}{i} b^{p-i} cp^\ell$ and $p^{\ell+1} \mid p^{i\ell}$ for $2 \le i \le p$, it follows that $a^p \equiv b^p \pmod{p^{\ell+1}}$. ∎

Proposition 48: Let p be an odd prime and $\ell \in \mathbb{N}$ with $\ell \ge 2$. Then for $a \in \mathbb{Z}$, we have

$$(1 + ap)^{p^{\ell-2}} \equiv 1 + ap^{\ell-1} \pmod{p^\ell}.$$

Proof: We prove the result by induction on ℓ. The result is immediate

for $\ell = 2$. Suppose that the result holds for some $\ell \in \mathbb{N}$ with $\ell \geq 2$ and we prove it for $\ell+1$. By proposition 47 and the induction hypothesis

$$\begin{aligned}(1+ap)^{p^{\ell-1}} &\equiv \left((1+ap)^{p^{\ell-2}}\right)^p \\ &\equiv (1+ap^{\ell-1})^p \\ &\equiv 1 + \binom{p}{1}ap^{\ell-1} + \cdots + \binom{p}{p}(ap^{\ell-1})^p \pmod{p^{\ell+1}}.\end{aligned}$$

Note that for $\ell \geq 2$ and $k \geq 3$, $2(\ell-1)+1 \leq 3(\ell-1) \leq k(\ell-1)$. It follows that

$$p^{2(\ell-1)+1} \mid (ap^{\ell-1})^k$$

for $k = 3, \ldots, p$. Also, we note that

$$\binom{p}{2}(ap^{\ell-1})^2 = \frac{p(p-1)}{2}(ap^{\ell-1})^2 = \frac{p-1}{2}a^2p^{2(\ell-1)+1}.$$

Since $\frac{p-1}{2} \in \mathbb{Z}$ as p is odd, it follows that

$$p^{2(\ell-1)+1} \mid \binom{p}{2}(ap^{\ell-1})^2.$$

Note that $2(\ell-1)+1 \geq \ell+1$ for $\ell \geq 2$. Thus $p^{\ell+1} \mid p^{2(\ell-1)+1}$. Thus we have

$$\begin{aligned}(1+ap)^{p^{\ell-1}} &\equiv 1 + \binom{p}{1}ap^{\ell-1} + \binom{p}{2}(ap^{\ell-1})^2 + \cdots + \binom{p}{p}(ap^{\ell-1})^p \\ &\equiv 1 + \binom{p}{1}ap^{\ell-1} \\ &\equiv 1 + ap^{\ell} \pmod{p^{\ell+1}}.\end{aligned}$$

By induction, the result holds. ∎

Proposition 49: If p is an odd prime, $\ell \geq 2$ and $a \in \mathbb{Z}$ with $(a,p)=1$, then $1+ap$ has order $p^{\ell-1}$ in $(\mathbb{Z}/p^{\ell}\mathbb{Z})^*$.

2015 11 06

Proof: Note that the group $(\mathbb{Z}/p\mathbb{Z})^*$ is of order $p^{\ell} - p^{\ell-1} = p^{\ell-1}(p-1)$. By theorem 48,

$$(1+ap)^{p^{\ell-2}} \equiv 1 + ap^{\ell-1} \pmod{p^{\ell}}.$$

Since $(a,p)=1$, we have

$$(1+ap)^{p^{\ell-2}} \not\equiv 1 \pmod{p^{\ell}}.$$

Then, by theorem 48 again,

$$(1+ap)^{p^{\ell-1}} \equiv 1 + ap^{\ell} \pmod{p^{\ell+1}}.$$

Thus $1+ap$ has order $p^{\ell-1}$ in $(\mathbb{Z}/p\mathbb{Z})^*$. ∎

Theorem 50: Let p be an odd prime and $\ell \in \mathbb{N}$ with $\ell \geq 2$. Then $(\mathbb{Z}/p^\ell\mathbb{Z})^*$ is a cyclic group.

Proof: By theorem 46, there exists a primitive root g modulo p. Note that

$$(g+p)^{p-1} = g^{p-1} + \binom{p-1}{1} g^{p-2} p + \binom{p-1}{2} g^{p-3} p^2 + \cdots + \binom{p-1}{p-1} p^{p-1}.$$

If we assume that $g^{p-1} \equiv 1 \pmod{p^2}$ then

$$(g+p)^{p-1} \equiv 1 + \binom{p-1}{1} g^{p-2} p \pmod{p^2}.$$

Since $p \nmid (p-1)$ and $(g,p)=1$, we see that

$$(g+p)^{p-1} \not\equiv 1 \pmod{p^2}.$$

Thus at least one of g^{p-1} and $(g+p)^{p-1}$ is not congruent to 1 modulo p^2.

Claim: If $g^{p-1} \not\equiv 1 \pmod{p^2}$, then g is a primitive root modulo p^ℓ.

Verification: Suppose g has order m in $(\mathbb{Z}/p^\ell\mathbb{Z})^*$. Since

$$|(\mathbb{Z}/p^{\ell-1}\mathbb{Z})| = p^{\ell-1}(p-1),$$

we have $m \mid p^{\ell-1}(p-1)$. Write $m = dp^s$ where $d \mid (p-1)$ and $0 \leq s \leq \ell-1$. By Fermat's little theorem, $g^p \equiv g \pmod{p}$. Thus $g^{p^s} \equiv g \pmod{p}$, for $s \in \mathbb{N}$. Since $g^m \equiv 1 \pmod{p^\ell}$ and thus $g^m \equiv 1 \pmod{p}$, we have

$$g^d \equiv (g^{p^s})^d \equiv g^m \equiv 1 \pmod{p}.$$

Since g is a primitive root modulo p, we have $(p-1) \mid d$. Thus $d = p-1$. Since $g^{p-1} \equiv 1 \pmod{p}$ and $g^{p-1} \not\equiv 1 \pmod{p^2}$, there is $a \in \mathbb{Z}$ with $(a,p)=1$ such that $g^{p-1} \equiv 1 + ap \pmod{p^2}$. By theorem 49, $1+ap$ has order $p^{\ell-1}$ in $(\mathbb{Z}/p^\ell\mathbb{Z})^*$. Thus g has order $(p-1)p^\ell$, which implies that $(\mathbb{Z}/p^\ell\mathbb{Z})^*$ is cyclic. □

This completes the proof, as without loss of generality, $g^{p-1} \not\equiv 1 \pmod{p^2}$. ■

Theorem 51: Let $\ell \in \mathbb{N}$. Then:

(1) if $\ell = 1, 2$ then $(\mathbb{Z}/p^\ell\mathbb{Z})^*$ is cyclic;

(2) if $\ell \geq 3$ then

$$(\mathbb{Z}/2^\ell\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/2^{\ell-2}\mathbb{Z}).$$

In particular,

$$(\mathbb{Z}/2^\ell\mathbb{Z})^* = \{(-1)^a 5^b + 2^\ell\mathbb{Z} \,;\, a \in \{0,1\},\ b \in \{0,1,\ldots,2^{\ell-2}-1\}\}$$

Proof: (1) One can verify that $(\mathbb{Z}/2\mathbb{Z})^*$ and $(\mathbb{Z}/4\mathbb{Z})^*$ are cyclic.
(2) Suppose $\ell \geq 3$.
Claim 1: For $\ell \geq 3$, $5^{2^{\ell-3}} \equiv 1 + 2^{\ell-1} \pmod{2^\ell}$.
Verification: By induction on ℓ. For $\ell = 3$, we have $5 \equiv 1 + 2^2 \pmod{2^3}$ as required. Suppose that the above congruence holds for some $\ell \geq 3$ and we prove the result for $\ell+1$. Write $5^{2^{\ell-3}} = 1 + 2^{\ell-1} + k2^\ell$ for some $k \in \mathbb{Z}$. It follows that

$$\begin{aligned} 5^{2^{\ell-2}} &= (1 + 2^{\ell-1} + k2^\ell)^2 \\ &= 1 + (2^{\ell-1})^2 + 2 \cdot 2^{\ell-1} + 2k2^\ell + 2 \cdot 2^{\ell-1} k2^\ell + k^2 (2^\ell)^2 \\ &= 1 + 2^\ell + k2^{\ell+1} + 2^{2\ell-1} + k2^{2\ell} + k^2 2^{2\ell}. \end{aligned}$$

Note that $2(\ell-1) \geq \ell+1$ for $\ell \geq 3$. Thus we have

$$5^{2^{\ell-2}} \equiv 1 + 2^\ell \pmod{2^{\ell+1}}.$$

By induction, the claim holds. □
Thus $5^{2^{\ell-3}} \not\equiv 1 \pmod{2^\ell}$, and $5^{2^{\ell-2}} \equiv 1 \pmod{2^\ell}$. Thus 5 has order $2^{\ell-2}$ in $(\mathbb{Z}/2^\ell\mathbb{Z})^*$.
Claim 2: For $\ell \geq 3$, the numbers $(-1)^a 5^b$ with $a \in \{0,1\}$ and $b \in \{0, \dots, 2^{\ell-2}-1\}$ are distinct modulo 2^ℓ.
Verification: Suppose that $(-1)^{a_1} 5^{b_1} \equiv (-1)^{a_2} 5^{b_2} \pmod{2^\ell}$ with $a_i \in \{0,1\}$ and $b_i \in \{0, \dots, 2^{\ell-2}-1\}$ for $i \in \{1,2\}$. Then $(-1)^{a_1} 5^{b_1} \equiv (-1)^{a_2} 5^{b_2} \pmod 4$. Since $5 \equiv 1 \pmod 4$, we see that $(-1)^{a_1} \equiv (-1)^{b_1} \pmod 4$. Thus $a_1 = a_2$. We now have $5^{b_1} \equiv 5^{b_2} \pmod{2^\ell}$. Since 5 has order $2^{\ell-2}$ in $(\mathbb{Z}/2^\ell\mathbb{Z})^*$ and $0 \leq b_i < 2^{\ell-2}$, it follows that $b_1 = b_2$. □
Since

$$(\mathbb{Z}/2^\ell\mathbb{Z})^* = \{(-1)^a 5^b ; a \in \{0,1\}, b \in \{0, \dots, 2^{\ell-2}-1\}\},$$

it follows that

$$(\mathbb{Z}/2^\ell\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\ell-2}\mathbb{Z}).$$

■

2015 11 09

Theorem 52: The group $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic (i.e. it has a primitive root) if and only if $n = 1, 2, 4, p^\ell$ and $2p^\ell$ with p an odd prime and $\ell \in \mathbb{N}$.

Proof: Let $n = 2^{\ell_0} p_1^{\ell_1} \cdots p_r^{\ell_r}$ where $\ell_0 \in \mathbb{N} \cup \{0\}$, $\ell_1, \dots, \ell_r \in \mathbb{N}$, and $p_1, \dots, p_r$ are distinct odd primes. Then by theorem 42,

$$(\mathbb{Z}/n\mathbb{Z})^* \simeq (\mathbb{Z}/2^{\ell_0}\mathbb{Z})^* \times (\mathbb{Z}/p_1^{\ell_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_r^{\ell_r}\mathbb{Z})^*.$$

By Theorem 46, $(\mathbb{Z}/p_i^{\ell_i}\mathbb{Z})^*$ is cyclic $(1 \le i \le r)$. By Theorem 51, $(\mathbb{Z}/2^{\ell_0}\mathbb{Z})^*$ is cyclic for $0 \le \ell_0 \le 2$ and is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\ell_0-2}\mathbb{Z}$ for $\ell \ge 3$. Thus, the order of any element of $(\mathbb{Z}/n\mathbb{Z})^*$ is a divisor of

$$\lambda(n) = \operatorname{lcm}(b, \varphi(p_1^{\ell_1}), \dots, \varphi(p_r^{\ell_r}))$$

where

$$b = \begin{cases} \varphi(2^{\ell_0}) & \text{if } 0 \le \ell_0 \le 2, \\ \frac{1}{2}\varphi(2^{\ell_0}) & \text{if } \ell_0 \ge 3. \end{cases}$$

Note that $2 \mid \varphi(p_i^{\ell_i})$ $(1 \le i \le r)$. It follows that

$$\lambda(n) < \varphi(2^{\ell_0})\varphi(p_1^{\ell_1}) \cdots \varphi(p_r^{\ell_r})$$

except in the cases $n = 1, 2, 4, p_i^{\ell}$ and $2p_i^{\ell}$. Since $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic if and only if

$$\lambda(n) = \varphi(2^{\ell_0})\varphi(p_1^{\ell_1}) \cdots \varphi(p_r^{\ell_r}),$$

the result follows. ∎

Def) The number

$$\lambda(n) = \operatorname{lcm}(b, \varphi(p_1^{\ell_1}), \dots, \varphi(p_r^{\ell_r}))$$

is called the <u>universal exponent of n</u>.

Theorem 53: For $n \in \mathbb{N}$, let $\lambda(n)$ be its universal exponent. Then for any $a \in \mathbb{Z}$ with $(a,n) = 1$, we have

$$a^{\lambda(n)} \equiv 1 \pmod{n}.$$

Remark: Euler's theorem states that for any $a \in \mathbb{Z}$ with $(a,n) = 1$ we have $a^{\varphi(n)} \equiv 1 \pmod{n}$. The above gives a strengthening of Euler's theorem

Remark: Given a prime p one can ask for an upper bound for the smallest positive integer b which is a primitive root mod p. It was proved by Hua that

$$b < 2^{\omega(p-1)+1}\sqrt{p}.$$

Theorem 54: If p is a prime of the form $4q+1$ with q an odd prime, then 2 is a primitive root mod p.

Proof: Let m be the order of 2 mod p. By Fermat's little theorem, $m|(p-1)$ and thus $m|4q$. It follows that $m = 1, 2, 4, q, 2q,$ or $4q$. Since p is a prime of the form $4q+1$ with q an odd prime, we have $p = 13$ or $p > 20$. Thus $m \neq 1, 2, 4$. Also, by Euler's Criterion,

$$2^{2q} \equiv 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod{p}.$$

On the other hand, by corollary 38, since q is odd,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(4q+1)^2-1}{8}} = (-1)^{2q^2+q} = -1.$$

Thus $m \neq q, 2q$ because

$$2^{2q} \equiv -1 \pmod{p}.$$

It follows that $m = 4q = p-1$, i.e. 2 is a primitive root mod 2. ∎

Let $k, \ell \in \mathbb{N}$ with $(k, \ell) = 1$. Dirichlet's theorem states that there are infinitely many primes p with $p \equiv \ell \pmod{k}$. To prove this theorem, we'll introduce later the notion of L-functions. However, for many pairs (k, ℓ), we can prove Dirichlet's theorem by elementary means. For example, on assignment 1, we showed that there are infinitely many primes p with $p \equiv 5 \pmod{6}$, i.e. $(k, \ell) = (6, 5)$.

2015 11 11

Theorem 55: Let $n \in \mathbb{N}$. There are infinitely many primes p with

$$p \equiv 1 \pmod{n}.$$

Proof (due to Birkhoff and Vandiver, 1904): Let $a \in \mathbb{N}$ with $a > 2$ and

$$\zeta_n = e^{\frac{2\pi i}{n}}.$$

Consider $\Phi_n(a)$, the cyclotomic polynomial evaluated at a, i.e.

$$\Phi_n(a) = \prod_{\substack{j=1 \\ (n,j)=1}}^{n} \left(a - \zeta_n^j\right).$$

We recall that $\Phi_n(x) \in \mathbb{Z}[x]$ and

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Claim: If p is a prime dividing $\Phi_n(a)$, then $p|n$ or $p \equiv 1 \pmod{n}$.
Verification: Note that $p|(a^n - 1)$ and thus $p \nmid a$. There are two cases.
(1) If $p \nmid (a^d - 1)$ for all $d|n$ with $d \neq n$. Then the order of a mod p

is n. By Fermat's little theorem, $n \mid (p-1)$ and $p \equiv 1 \pmod{n}$.
(2) Suppose that $p \mid (a^d - 1)$ for some $d \mid n$ with $d \neq n$. Note that

$$\Phi_n(x) \Big| \left(\frac{x^n - 1}{x^d - 1} \right)$$

in $\mathbb{Z}[x]$. Since $p \mid \Phi_n(a)$, it follows that

$$p \Big| \frac{a^n - 1}{a^d - 1}.$$

We have

$$a^n = (1 + (a^d - 1))^{\frac{n}{d}} = 1 + \frac{n}{d}(a^d - 1) + \binom{n/d}{2}(a^d - 1)^2 + \cdots.$$

Thus

$$\frac{a^n - 1}{a^d - 1} = \frac{n}{d} + \binom{n/d}{2}(a^d - 1) + \cdots.$$

Since

$$p \Big| \left(\frac{a^n - 1}{a^d - 1} \right) \quad \text{and} \quad p \mid (a^d - 1),$$

we conclude that $p \mid \frac{n}{d}$. Thus we have $p \mid n$. This completes the proof of the claim. □

We are now ready to prove the theorem. Suppose that there are only finitely many primes $p_1, \ldots, p_r$ with $p_j \equiv 1 \pmod{n}$ $(1 \leq j \leq r)$. Write

$$\Phi_n(x) = x^{\varphi(n)} + \cdots + \pm 1.$$

Consider

$$\Phi_n(np_1 p_2 \cdots p_r m).$$

We see that

$$(\Phi_n(np_1 p_2 \cdots p_r m), n) = 1.$$

Also,

$$p_j \nmid \Phi_n(np_1 \cdots p_r m)$$

$(1 \leq j \leq r)$. Letting $m \to \infty$, we see that for sufficiently large m,

$$\Phi_n(np_1 \cdots p_r m) \geq 2.$$

Thus it has a prime divisor p, which is not equal to $p_1, \ldots, p_r$. By the claim, we have either $p \equiv 1 \pmod{n}$ or $p \mid n$. Since

$$(\Phi_n(np_1 \cdots p_r m), n) = 1,$$

we have $p \nmid n$. Thus $p \equiv 1 \pmod{n}$. However, $p \notin \{p_1, \ldots, p_r\}$, contradiction. ■