Solutions to Ireland, Rosen "A Classical Introduction to Modern Number Theory"

Richard Ganaye

September 18, 2019

Chapter 4

Ex. 4.1 *Show that 2 is a primitive root modulo 29.*

Proof. Let $p = 29 : p - 1 = 2^2 \times 7$.

$2^4 = 16 \not\equiv 1[29]$

$2^{14} = 4^7 = 4 \times 16^3 = 64 \times 256 \equiv 6 \times (-34) = -204 \equiv 86 = 3 \times 29 - 1 \equiv -1[29]$

$2^{28} \equiv 1[29]$ and $2^d \not\equiv 1$ if $d \mid 28, d < 28$, hence 2 is a primitive element modulo 29. $\square$

Ex. 4.2 *Compute all primitive roots for $p = 11, 13, 17$, and 19.*

Proof. • $p = 11$. Then $p - 1 = 10 = 2 \times 5$.

$2^2 = 4 \not\equiv 1 \pmod{11}$, and $2^5 = 32 \equiv -1 \not\equiv 1 \pmod{11}$, so 2 is a primitive element modulo 11.

The other primitive elements modulo 11 are congruent to the powers $2^i, i \wedge 10 = 1, 1 \leq i < 10$, namely $2, 2^3, 2^7, 2^9$.

$2^7 \equiv 7 \pmod{11}, 2^9 \equiv 6 \pmod{11}$, so

$\{\overline{2}, \overline{8}, \overline{7}, \overline{6}\}$ is the set of the generators of $U(\mathbb{Z}/11\mathbb{Z})$.

Similarly :

• $p = 13 : \{2, 6, 11, 7\}$ is the set of the generators of $U(\mathbb{Z}/13\mathbb{Z})$.

• $p = 17 : \{3, 10, 5, 11, 14, 7, 12, 6\}$ is the set of the generators of $U(\mathbb{Z}/17\mathbb{Z})$.

• $p = 19 : \{2, 13, 14, 15, 3, 10\}$ is the set of the generators of $U(\mathbb{Z}/19\mathbb{Z})$.

I obtain these results with the direct orders in S.A.G.E. :

```
p = 19; Fp = GF(p); a = Fp.multiplicative_generator()
print([a^k for k in range(1,p) if gcd(k,p-1) == 1])
```

$\square$

Ex. 4.3 *Suppose that a is a primitive root modulo p^n, p an odd prime. Show that a is a primitive root modulo p.*

Proof. Suppose that a is a primitive root modulo p^n : then $\overline{a}$ is a generator of $U(\mathbb{Z}/p^n\mathbb{Z})$.

If a was not a primitive root modulo p, $\overline{a}$ is not a generator of $U(\mathbb{Z}/p\mathbb{Z})$, so there exists $b \in \mathbb{Z}, b \wedge p = 1$ such that $a^k \not\equiv b \pmod{p}$ for all $k \in \mathbb{Z}$. A fortiori $a^k \not\equiv b \pmod{p^n}$, and $b \wedge p^n = 1$, so $\overline{b} \in U(\mathbb{Z}/p^n\mathbb{Z})$ and $\overline{b} \notin \langle \overline{a} \rangle$ in $U(\mathbb{Z}/p^n\mathbb{Z})$, in contradiction with the hypothesis. So a is a primitive root modulo p.

(the reasoning on the orders of a, modulo p and modulo p^n, is possible, but not so easy.) $\square$

Ex. 4.4 *Consider a prime p of the form $4t+1$. Show that a is a primitive root modulo p iff $-a$ is a primitive root modulo p.*

Proof. Solution 1.

As. $p-1$ is even, $(-a)^{p-1} = a^{p-1} \equiv 1 \pmod p$.

If $(-a)^n \equiv 1 \pmod p$, with $n \in \mathbb{N}$, then $a^n \equiv (-1)^n \pmod p$.

If n is odd, then $a^n \equiv -1, a^{2n} \equiv 1 \pmod p$. As a is a primitive root modulo p, $p-1 \mid 2n$, $2t \mid n$, so n is even : this is a contradiction.

Consequently, n is even, and $a^n \equiv 1 \pmod p$, so $p-1 \mid n$, so the least $n \in \mathbb{N}^*$ such that $a^n \equiv 1 \pmod p$ is $p-1$: the order of a modulo p is $p-1$, a is a primitive root modulo p.

Reciprocally, if $-a$ is a primitive root modulo p, we apply the previous result at $-a$ to to obtain that $-(-a) = a$ is a primitive root.

Solution 2.

Let $p-1 = 2^{a_0} p_1^{a_1} \cdots p_k^{a_k}$ the decomposition of $p-1$ in prime factors.

As p_i is odd for $i = 1, 2, \cdots k$, $(p-1)/p_i$ is even, and a is primitive, so

$$\begin{aligned} (-a)^{(p-1)/p_i} &= a^{(p-1)/p_i} \not\equiv 1 \pmod p, \\ (-a)^{(p-1)/2} &= (-a)^{2k} = a^{2k} = a^{(p-1)/2} \not\equiv 1 \pmod p. \end{aligned}$$

So the order of a is $p-1$ modulo p (see Ex. 4.8) : a is a primitive element modulo p. □

Ex. 4.5 *Consider a prime p of the form $4t+3$. Show that a is a primitive root modulo p iff $-a$ has order $(p-1)/2$.*

Proof. Let a a primitive root modulo p.

As $a^{p-1} \equiv 1 \pmod p$, $p \mid (a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1)$, so $p \mid a^{(p-1)/2} - 1$ or $p \mid a^{(p-1)/2} + 1$. As a is a primitive root modulo p, $a^{(p-1)/2} \not\equiv 1 \pmod p$, so

$$a^{(p-1)/2} \equiv -1 \pmod p.$$

Hence $(-a)^{(p-1)/2} = (-1)^{2t+1} a^{(p-1)/2} \equiv (-1) \times (-1) = 1 \pmod p$.

Suppose that $(-a)^n \equiv 1 \pmod p$, with $n \in \mathbb{N}$.

Then $a^{2n} = (-a)^{2n} \equiv 1 \pmod p$, so $p-1 \mid 2n$, $\frac{p-1}{2} \mid n$.

So $-a$ has order $(p-1)/2$ modulo p.

Reciprocally, suppose that $-a$ has order $(p-1)/2 = 2t+1$ modulo p. Let $2, p_1, \ldots p_k$ the prime factors of $p-1$, where p_i are odd.

$a^{(p-1)/2} = a^{2t+1} = -(-a)^{2t+1} = -(-a)^{(p-1)/2} \equiv -1$, so $a^{(p-1)/2} \not\equiv 1 \pmod 2$.

As $p-1$ is even, $(p-1)/p_i$ is even, so

$a^{(p-1)/p_i} = (-a)^{(p-1)/p_i} \not\equiv 1 \pmod p$ (since $-a$ has order $p-1$).

So the order of a is $p-1$ (see Ex. 4.8) : a is a primitive root modulo p. □

Ex. 4.6 *If $p = 2^{2^n} + 1$ is a Fermat prime, show that 3 is a primitive root modulo p.*

Proof. Solution 1 (with quadratic reciprocity).

Write $p = 2^k + 1$, with $k = 2^n$.

We suppose that $n > 0$, so $k \geq 2, p \geq 5$. As p is prime, $3^{p-1} \equiv 1 \pmod p$.

In other words, $3^{2^k} \equiv 1 \pmod p$: the order of 3 is a divisor of 2^k, a power of 2.

3 has order 2^k modulo p iff $3^{2^{k-1}} \not\equiv 1 \pmod p$. As $\left(3^{2^{k-1}}\right)^2 \equiv 1 \pmod p$, where p is prime, this is equivalent to $3^{2^{k-1}} \equiv -1 \pmod p$, which remains to prove.

$3^{2^{k-1}} = 3^{(p-1)/2} \equiv \left(\frac{3}{p}\right) \pmod p$.

As the result is true for $p = 5$, we can suppose $n \ge 2$. From the law of quadratic reciprocity :

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{(p-1)/2} = (-1)^{2^{k-1}} = 1.$$

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

$$\begin{aligned} p = 2^{2^n} + 1 &\equiv (-1)^{2^n} + 1 \pmod 3 \\ &\equiv 2 \equiv -1 \pmod 3, \end{aligned}$$

so $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = -1$, that is to say

$$3^{2^{k-1}} \equiv -1 \pmod p.$$

The order of 3 modulo $p = 2^{2^n} + 1$ is $p - 1 = 2^{2^n}$: 3 is a primitive root modulo p.

(On the other hand, if 3 is of order $p - 1$ modulo p, then p is prime, so

$$F_n = 2^{2^n} + 1 \text{ is prime} \iff 3^{(F_n-1)/2} = 3^{2^{2^n-1}} \equiv -1 \pmod{F_n}.)$$

Solution 2 (without quadratic reciprocity, with the hint of chapter 4).

As above, if if we suppose that 3 is not a primitive root modulo p, then $3^{2^{n-1}} \equiv 1 \pmod p$, so $n \ge 2$, and $(-3)^{(p-1)/2} = 3^{2^{n-1}} \equiv 1 \pmod p$, so -3 is a square modulo p : there exists $a \in \mathbb{Z}$ such that $-3 \equiv a^2 \pmod p$.

As $2 \wedge p = 1$, there exists $u \in \mathbb{Z}$ such that $2u \equiv -1 + a \pmod p$ ($\overline{u}$ is similar to $\omega = \frac{-1+i\sqrt{3}}{2} \in \mathbb{C}$). Then

$$\begin{aligned} 8u^3 &\equiv (-1 + a)^3 \\ &\equiv -1 + 3a - 3a^2 + a^3 \\ &\equiv -1 + 3a + 9 - 3a \\ &\equiv 8 \pmod p \end{aligned}$$

As $p \wedge 2 = p \wedge 8 = 1, u^3 \equiv 1 \pmod p$. Moreover, if $u \equiv 1 \pmod 3$, then $a \equiv 3 \pmod p$, $-3 \equiv 9 \pmod p, p \mid 12$, so $p = 2$ or $p = 3$, in contradiction with $p \ge 5$. So the order of u modulo p is 3 : $(\mathbb{Z}/p\mathbb{Z})^*$ contains an element $\overline{u}$ of order 3. So $3 \mid p - 1$, $p \equiv 1 \pmod 3$, but $p \equiv (-1)^{2^n} + 1 \equiv 2 \equiv -1 \pmod 3$: this is a contradiction, so 3 is a primitive root modulo $p = 2^{2^n} + 1$. □

Ex. 4.7 *Suppose that p is a prime of the form $8t + 3$ and that $q = (p - 1)/2$ is also a prime. Show that 2 is a primitive root modulo p.*

Proof. The first examples of such couples (q, p) are $(5, 11), (29, 59), (41, 83), (53, 107), (89, 179)$.

$p = 2q + 1 = 8t + 3$ and p, q are prime numbers.

From Fermat's little theorem, $2^{p-1} \equiv 1 \pmod p$, so $2^{2q} \equiv 1 \pmod p$.

The order of 2 modulo p divides $2q$: to prove that the order of 2 is $2q = p - 1$, it is suffisant to prove

$$2^2 \not\equiv 1 \pmod p, \quad 2^q \not\equiv 1 \pmod p.$$

If $2^2 \equiv 1 \pmod p$, then $p \mid 3$, $p = 3$ and $q = 1$: q is not a prime, so $2^2 \not\equiv 1 \pmod p$.

If $2^q = 2^{(p-1)/2} \equiv 1 \pmod p$, then 2 is a square modulo p (prop. 4.2.1) : there exists $a \in \mathbb{Z}$ such that $2 \equiv a^2 \pmod p$.

From the complementary case of law of quadratic reciprocity (see next chapter, prop. 5.1.3), 2 is a square modulo p iff

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

Yet $p \equiv 3 \pmod 8$, so $p^2 \equiv 1 \pmod{16}$, $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = -1$, so 2 is not a square modulo p. This is a contradiction, so $2^q \not\equiv 1 \pmod p$: 2 is a primitive root modulo p. □

Ex. 4.8 *Let p be an odd prime. Show that a is a primitive root modulo p iff $a^{(p-1)/q} \not\equiv 1 \pmod p$ for all prime divisors q of $p-1$.*

Proof. • If a is a primitive root, then $a^k \not\equiv 1$ for all $k, 1 \le k < p-1$, so $a^{(p-1)/q} \not\equiv 1 \pmod p$ for all prime divisors q of $p-1$.

• In the other direction, suppose $a^{(p-1)/q} \not\equiv 1 \pmod p$ for all prime divisors q of $p-1$.

Let δ the order of a, and $p-1 = q_1^{a_1} q_2^{a_2} \cdots q_k^{a_k}$ the decomposition of $p-1$ in prime factors. As $\delta \mid p-1, \delta = q_1^{b_1} p_2^{b_2} \cdots q_k^{b_k}$, with $b_i \le a_i, i = 1, 2, \ldots, k$. If $b_i < a_i$ for some index i, then $\delta \mid (p-1)/q_i$, so $a^{(p-1)/q_i} \equiv 1 \pmod p$, which is in contradiction with the hypothesis. Thus $b_i = a_i$ for all i, and $\delta = q-1$: a is a primitive root modulo p. □

Ex. 4.9 *Show that the product of all the primitive roots modulo p is congruent to $(-1)^{\phi(p-1)}$ modulo p.*

Proof. Here we suppose p prime, $p > 2$. Let g a primitive root modulo p. $U(\mathbb{Z}/p\mathbb{Z})$ is cyclic, generated by $\overline{g}$:

$$U(\mathbb{Z}/p\mathbb{Z}) = \{\overline{1}, \overline{g}, \overline{g}^2, \ldots, \overline{g}^{p-2}\}, \qquad \overline{g}^{p-1} = \overline{1}.$$

$\overline{g}^k$ is a primitive element iff $k \wedge (p-1) = 1$, so the product of primitive elements in $U(\mathbb{Z}/p\mathbb{Z})$ is

$$\overline{P} = \prod_{\substack{k \wedge (p-1) = 1 \\ 1 \le k < p-1}} \overline{g}^k.$$

so $\overline{P} = \overline{g}^S$, where $S = \sum_{\substack{k \wedge (p-1) = 1 \\ 1 \le k < p-1}} k$.

From Ex. 2.22, we know that for $n \ge 2$,

$$\sum_{\substack{k \wedge n = 1 \\ 1 \le k < n}} k = \frac{1}{2} n \phi(n).$$

So $S = \sum_{\substack{k \wedge (p-1) = 1 \\ 1 \le k < p-1}} k = \frac{1}{2}(p-1)\phi(p-1)$.

As $p > 2$, $p-1$ is even. $(\overline{g}^{(p-1)/2})^2 = \overline{g}^{p-1} = \overline{1}$, and $\overline{g}^{(p-1)/2} \ne \overline{1}$. As $\mathbb{Z}/p\mathbb{Z}$ is a field, $\overline{g}^{(p-1)/2} = -\overline{1}$.

Thus $\overline{P} = (-\overline{1})^{\phi(p-1)}$: so the product P of all the primitive roots modulo p is such that

$$P \equiv (-1)^{\phi(p-1)} \pmod p.$$

□

Ex. 4.10 *Show that the sum of all the primitive roots modulo p is congruent to $\mu(p-1)$ modulo p.*

Proof. Notation : $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is the field with p elements, $|x|$ the multiplicative order of an element $x \in \mathbb{F}_p^*$, $\mathbb{N}^* = \{1, 2, 3, \ldots\}$.

Let

$$\psi : \left\{ \begin{array}{ccc} \mathbb{N}^* & \to & \mathbb{F}_p \\ n & \mapsto & \psi(n) = \displaystyle\sum_{d \in \mathbb{F}_p^*, |d| = n} d \end{array} \right.$$

$\psi(n)$ is the sum of the elements with order n in $\mathbb{F}_p^*$. So $\psi(n) = 0$ if $n \nmid p-1$, and $S = \psi(p-1)$ is the sought sum of all the primitive roots modulo p.

We compute for all $n \in \mathbb{N}^*$

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

$f(n)$ is the sum of elements whose order divides n, in other worlds the sum of the roots of $x^n - 1$. This sum is, up to the sign, the coefficient of x^{n-1}, so is null, except in the case $n = 1$, where the sum of the unique root 1 of $x - 1$ is 1. So

$$f(1) = 1, \qquad \forall n > 1, f(n) = 0,$$

($f = \chi_{\{1\}}$ is the characteristic function of $\{1\}$).

From the Möbius inversion formula, for all $n \in \mathbb{N}^*, \psi(n) = \sum_{d|m} \mu\left(\frac{n}{d}\right) f(d)$, so

$$\psi(p-1) = \sum_{d|p-1} \mu\left(\frac{p-1}{d}\right) f(d) = \mu(p-1).$$

Conclusion :

$$S = \sum_{d \in \mathbb{F}_p^*, |d| = p-1} d = \mu(p-1) :$$

the sum of all the primitive roots modulo p is congruent to $\mu(p-1)$ modulo p. $\square$

Ex. 4.11 *Prove that $1^k + 2^k + \ldots + (p-1)^k \equiv 0 \pmod p$ if $p-1 \nmid k$, and $-1 \pmod p$ if $p-1 \mid k$.*

Proof. Let $S_k = 1^k + 2^k + \cdots + (p-1)^k$.

Let g a primitive root modulo p : $\overline{g}$ a generator of $\mathbb{F}_p^*$.

As $(\overline{1}, \overline{g}, \overline{g}^2, \ldots, \overline{g}^{p-2})$ is a permutation of $(\overline{1}, \overline{2}, \ldots, \overline{p-1})$,

$$\begin{aligned} \overline{S_k} &= \overline{1}^k + \overline{2}^k + \cdots + \overline{p-1}^k \\ &= \sum_{i=0}^{p-2} \overline{g}^{ki} = \left\{ \begin{array}{lll} \overline{p-1} = -\overline{1} & \text{if} & p-1 \mid k \\ \frac{\overline{g}^{(p-1)k} - 1}{\overline{g}^k - 1} = \overline{0} & \text{if} & p-1 \nmid k \end{array} \right. \end{aligned}$$

since $p-1 \mid k \iff \overline{g}^k = \overline{1}$.

Conclusion :

$$\begin{aligned} 1^k + 2^k + \cdots + (p-1)^k &\equiv 0 \pmod p \text{ if } p-1 \nmid k \\ 1^k + 2^k + \cdots + (p-1)^k &\equiv -1 \pmod p \text{ if } p-1 \mid k \end{aligned}$$

$\square$

Ex. 4.12 *Use the existence of a primitive root to give another proof of Wilson's theorem*$(p-1)! \equiv -1 \pmod p$.

Proof. As the result is trivial if $p = 2$, we suppose that p is an odd prime.

Let g a primitive root modulo p : $\overline{g}$ a generator of $\mathbb{F}_p^*$.

As $(\overline{g}^{(p-1)/2})^2 = \overline{g}^{p-1} = \overline{1}$, and $\overline{g}^{(p-1)/2} \neq 1$ in the field $\mathbb{F}_p^*$, then $\overline{g}^{(p-1)/2} = -1$, and $(\overline{1}, \overline{g}, \overline{g}^2, \ldots, \overline{g}^{p-2})$ is a permutation of $(\overline{1}, \overline{2}, \ldots, \overline{p-1})$, so

$$\begin{aligned}
\overline{(p-1)!} &= \prod_{k=0}^{p-2} \overline{g}^k \\
&= \overline{g}^{\sum_{k=0}^{p-2} k} \\
&= \overline{g}^{(p-2)(p-1)/2} \\
&= \left(\overline{g}^{(p-1)/2}\right)^{p-2} \\
&= (-\overline{1})^{p-2} \\
&= -1.
\end{aligned}$$

Hence $(p-1)! \equiv -1 \pmod p$ for each prime p. □

Ex. 4.13 *Let G be a finite cyclic group and $g \in G$ a generator. Show that all the other generators are of the form g^k, where $(k, n) = 1$, n being the order of G.*

Proof. Suppose $G = \langle g \rangle$, with $\mathrm{Card}\, G = n$, so the order of g is n.

Let x another generator of G, then $x = g^k$, and $g = x^l$, $k, l \in \mathbb{Z}$, so $g = g^{kl}, g^{kl-1} = e : n \mid kl - 1$, then $kl - 1 = qn, q \in \mathbb{Z}$, so $n \wedge k = 1$.

Reciprocally, if $u \wedge k = 1$, there exist $u, v \in \mathbb{Z}$ such that $un + vk = 1$, so $g = g^{un+vk} = (g^n)^u (g^k) v = x^v \in \langle x \rangle$, so $G \subset \langle x \rangle$, $G = \langle x \rangle$: x is a generator of G.

Conclusion : if g is a generator of G, all the other generators are the elements g^k, where $k \wedge n = 1$, $n = |G|$. □

Ex. 4.14 *Let A be a finite abelian group and $a, b \in A$ elements of order m and n, respectively. If $(m, n) = 1$, prove that ab has order mn.*

Proof. Suppose $|a| = m, |b| = n, m \wedge n = 1$.

• If $(ab)^k = e$, then $a^k = b^{-k}$, so $a^{kn} = b^{-kn} = (b^n)^{-k} = e$, so $m \mid kn$, with $m \wedge n = 1$, so $m \wedge k$.

Similarly, $b^{km} = a^{-km} = (a^m)^{-k} = e$, so $n \mid km, n \wedge m = 1 : n \mid k$.

As $n \mid k, m \mid k, n \wedge m = 1, nm \mid k$.

• Reciprocally, if $nm \mid k, nm = qnm, q \in \mathbb{Z}$, so $(ab)^k = a^k b^k = (a^m)^{qn} (b^n)^{qm} = e$.

$$\forall k \in \mathbb{Z},\ (ab)^k = e \iff nm \mid k.$$

So $|ab| = nm$. □

Ex. 4.15 *Let K be a field and $G \subset K^*$ a finite subgroup of the multiplicative group of K. Extend the arguments used in the proof of Theorem 4.1 to show that G is cyclic.*

Solution 1.

Proof. Let $n = |G|$. From Lagrange's theorem, $a^n = 1$ for all $a \in G$, so the polynomial $x^n - 1 \in K[x]$ has exactly n roots in G, and so

$$\forall x \in K, x \in G \iff x^n = 1.$$

If $d \mid n$, the polynomial $x^d - 1 \in K[x]$ has exactly d roots in K otherwise $x^n - 1 = (x^d - 1)g(x), g(x) \in K[x]$, and $\deg(g) = n - d$ has at most $n - d$ roots, so $x^n - 1$ would have less than n roots in K. As $x_0^d = 1 \Rightarrow x_0^n = 1$, all these roots are in G : $x^d - 1$ has d roots in G.

Let $\psi(d)$ the number of elements in G of order d ($\psi(d) = 0$ if $d \nmid n$). Then $\sum_{c|d} \psi(c) = d$. Applying the Möbius inversion theorem, $\psi(d) = \sum_{c|d} \mu(c)d/c = \Phi(d)$ (Prop. 2.2.5), in particular, $\psi(n) = \phi(n) > 1$ if $n > 2$. Since a group of order 2 is cyclic, we have shown in all cases the existence of an element of order n in G, so G is cyclic.

(variation : $\psi(d) = 0$ if there exists no element of order d, and $\psi(d) = \phi(d)$ otherwise : see Ex.4.13. So $\psi(d) \le \phi(d)$ for all $d \mid n$. As $\sum_{d|n} \psi(d) = \sum_{d|n} \phi(d) = n$, $\psi(d) = \phi(d)$ for all $d \mid n$. So there exists in G an element of order n, and G is cyclic.) □

Solution 2.

Proof. Let $n = |G| = p_1^{a_1} \cdots p_k^{a_k}$. From Lagrange's theorem, $y^n = 1$ for all $y \in G$.

$p(x) = x^{n/p_1} - 1 \in K[x]$ has at most $n/p_1 < n$ roots in K^*, a fortiori in G, so there exists $a \in G$ such that $a^{n/p_1} \ne 1$.

Let $c_1 = a^{n/p_1^{a_1}} = a^{p_2^{a_2} \cdots p_k^{a_k}}$. Then $c_1^{p_1^{a_1}} = 1$ and $c_1^{p_1^{a_1 - 1}} = a^{n/p_1} \ne 1$, so $|c_1| = p_1^{a_1}$.

Similarly, there exist $c_2, \ldots, c_k$ with respective orders $|c_i| = p_i^{a_i}$.

From exercise 4.14, we obtain by induction that $c = c_1 \cdots c_k$ has order $p_1^{a_1} \cdots p_k^{a_k} = n$, so G is cyclic. □

Ex. 4.16 *Calculate the solutions to* $x^3 \equiv 1 \pmod{19}$ *and* $x^4 \equiv 1 \pmod{17}$.

Proof. Here we note a the class of a in $\mathbb{Z}/p\mathbb{Z}$.

Let $x \in \mathbb{F}_{19}$. $x^3 - 1 = 0 \iff x - 1 = 0$ or $x^2 + x + 1 = 0$.

$$\begin{aligned} x^2 + x + 1 = 0 &\iff (x + 10) - 99 = 0 \\ &\iff (x + 10)^2 - 4 = 0 \\ &\iff (x + 8)(x + 12) = 0 \end{aligned}$$

So, for all $x \in \mathbb{Z}$,

$$x^3 \equiv 1 \pmod{19} \iff x \equiv 1, 7, 11 \pmod{19}.$$

Let $x \in \mathbb{F}_{17}$.

$$\begin{aligned} x^4 = 1 &\iff x^2 = 1 \text{ or } x^2 = -1 = 4^2 \\ &\iff x = \pm 1 \text{ or } x = \pm 4 \end{aligned}$$

So, for all $x \in \mathbb{Z}$,

$$x^4 \equiv 1 \pmod{17} \iff x \equiv -1, 1, -4, 4 \pmod{17}.$$

Alternatively, we can take primitives roots modulo 19 and 17.

2 is a primitive root modulo 19, Let $x = 2^k \in \mathbb{F}_{19}$.

$$\begin{aligned} x^3 = 1 &\iff 2^{3k} = 1 \\ &\iff 18 \mid 3k \\ &\iff 6 \mid k \\ &\iff x = 1, 2^6 = 7, 2^{12} = 11 \end{aligned}$$

3 is a primitive root modulo 17. Let $x = 3^k \in \mathbb{F}_{17}$.

$$\begin{aligned} x^4 = 1 &\iff 3^{4k} = 1 \\ &\iff 16 \mid 4k \\ &\iff 4 \mid k \\ &\iff x = 1, 3^4 = -4, 3^8 = -1, 3^{12} = 4 \end{aligned}$$

□

Ex. 4.17 *Use the fact that 2 is a primitive root modulo 29 to find the seven solutions to $x^7 \equiv 1 \pmod{29}$.*

Proof. Let $x \in \mathbb{Z}$, then $x \equiv 2^k \pmod{29}, k \in \mathbb{N}$.

$$\begin{aligned} x^7 \equiv 1 \pmod{29} &\iff 2^{7k} \equiv 1 \pmod{29} \\ &\iff 28 \mid 7k \\ &\iff 4 \mid k \end{aligned}$$

So the group cyclic S of the roots of $x^7 - 1$ in $\mathbb{F}_{29}$ are

$$S = \{1, 2^4, 2^8, 2^{12}, 2^{16}, 2^{20}, 2^{24}\},$$

$$S = \{1, 16, 24, 7, 25, 23, 20\}.$$

□

Ex. 4.18 *Solve the congruence $1 + x + \cdots + x^6 \equiv 0 \pmod{29}$.*

Proof. As $(1 + x + \cdots + x^6)(1 - x) = 1 - x^7$,

$$1 + x + \cdots + x^6 \equiv 0 \pmod{29} \iff \left\{ \begin{array}{rcll} x^7 & \equiv & 1 & \pmod{29} \\ x & \not\equiv & 1 & \pmod{29} \end{array} \right.$$

From Ex. 4.17, the solutions are congruent to $2^4, 2^8, 2^{12}, 2^{16}, 2^{20}, 2^{24}$ modulo 29. □

Ex. 4.19 *Determine the numbers a such that $x^3 \equiv a \pmod{p}$ is solvable for $p = 7, 11, 13$.*

Proof. (a) If $p = 7$, then $3 \mid p - 1, d = 3 \wedge (p - 1) = 3$. From Prop. 4.2.1,

$$\exists x \in \mathbb{Z},\ a \equiv x^3 \pmod{7} \iff a \equiv 0 \pmod{7} \text{ or } a^{(p-1)/3} = a^2 \equiv 1 \pmod{7}.$$

So the numbers a such that $x^3 \equiv a \pmod{7}$ is solvable are congruent at $0, 1, -1$ modulo 7.

(b) If $p = 11$, then $d = 3 \wedge (p-1) = 1$. With the same proposition,

$$\exists x \in \mathbb{Z},\ a \equiv x^3 \pmod{11} \iff a \equiv 0 \pmod{11} \text{ or } a^{p-1} = a^6 \equiv 1 \pmod{11}.$$

So all integers a are cube modulo 11, in only one way.

For an alternative proof, the application

$$f : \left\{ \begin{array}{ccc} \mathbb{F}_{11}^* & \to & \mathbb{F}_{11}^* \\ x & \mapsto & x^3 \end{array} \right.$$

f is a bijection. Indeed,

- f is a group homomorphism,
- $x^3 = 1 \Rightarrow (x^3)^7 = 1 \Rightarrow x = 1$ so $\ker(f) = \{1\}$,
- $f : \mathbb{F}_{11}^* \to \mathbb{F}_{11}^*$ is injective and $\mathbb{F}_{11}^*$ is finite, so f is bijective.

In $\mathbb{F}_{11}$, $0 = 0^3, 1 = 1^3, 2 = 7^3, 3 = 9^3, 4 = 5^3, 5 = 3^3, 6 = 8^3, 7 = 6^3, 8 = 2^3, 9 = 4^3, 10 = 10^3$.

(c) If $p = 13$, then $3 \mid p-1, 3 \wedge (p-1) = 3$, so

$$\begin{aligned} \exists x \in \mathbb{Z},\ a \equiv x^3 \pmod{13} &\iff a \equiv 0 \pmod{13} \text{ or } a^{(p-1)/3} = a^4 \equiv 1 \pmod{13} \\ &\iff a \equiv 0, 1, -1, 5, -5 \pmod{13} \end{aligned}$$

($5 \equiv 8^3 \pmod{13}$.)

□

Ex. 4.20 *Let p be a prime, and d a divisor of $p-1$. Show that dth powers form a subgroup of $U(\mathbb{Z}/p\mathbb{Z})$ of order $(p-1)/d$. Calculate this subgroup for $p = 11, d = 5$, for $p = 17, d = 4$, and for $p = 19, d = 6$.*

Proof. Here p is a prime number, and $d \mid p-1$. Let

$$f : \left\{ \begin{array}{ccc} \mathbb{F}_p^* & \to & \mathbb{F}_p^* \\ x & \to & x^d \end{array} \right.$$

Then f is a group homomorphism, and $\mathrm{im}(f)$ is the set of dth powers, and consequently is a subgroup of $U(\mathbb{F}_p) = \mathbb{F}_p^*$. $\ker(f)$ is the group of the roots of $x^d - 1$. As $d \mid p-1$, the polynomial $x^d - 1$ has exactly d roots (Prop. 4.1.2), so $|\ker(f)| = d$.

As $\mathrm{im}(f) \simeq \mathbb{F}_p^*/\ker(f)$,

$$|\mathrm{im}(f)| = |\mathbb{F}_p^*|/|\ker(f)| = (p-1)/d.$$

So there exist exactly $(p-1)/d$ dth powers in $(\mathbb{Z}/p\mathbb{Z})^*$.

From Prop. 4.2.1, as $d \mid p-1, d \wedge p-1$, for all $x \in \mathbb{F}_p^*$,

$$x \in \mathrm{im}(f) \iff x^{(p-1)/d} = 1.$$

So the group of dth powers is the group of the roots of $x^{(p-1)/d} - 1$.

- If $p = 11, d = 5$, $\mathrm{im}(f) = \{1, -1\}$.
- If $p = 17, d = 4$, $x \in \mathrm{im}(f) \iff x^4 = 1 : \mathrm{im}(f) = \{1, -1, 4, -4\}$.
- If $p = 19, d = 6$, $x \in \mathrm{im}(f) \iff x^3 = 1 : \mathrm{im}(f) = \{1, 7, 7^2 = 11\}$,

where $7 \equiv 2^6 \pmod{19}$.

□

Ex. 4.21 *If g is a primitive root modulo p, and $d|p-1$, show that $g^{(p-1)/d}$ has order d. Show also that a is a dth power iff $a \equiv g^{kd} \pmod p$ for some k. Do Exercises 16-20 making use of those observations.*

Proof. Let $x = \overline{g}^{(p-1)/d} \in \mathbb{F}_p^*$, where g is a primitive root modulo p. For all $k \in \mathbb{Z}$,

$$\begin{aligned} x^k = 1 &\iff g^{k\frac{p-1}{d}} = 1 \\ &\iff p-1 \mid k\frac{p-1}{d} \\ &\iff d \mid k \end{aligned}$$

So the ordre of $\overline{g}^{(p-1)/d}$ is d.

- If $\overline{a} = \overline{g}^{kd}$, then $\overline{a} = x^d$, where $x = \overline{g}^k$, so $\overline{a}$ is a dth power.
- If $\overline{a} \neq \overline{0}$ is a dth power, $\overline{a} = x^d, x \in \mathbb{F}_p^*$. As $x \in \langle \overline{g} \rangle$, $x = \overline{g}^k$, so $\overline{a} = \overline{g}^{kd}$.

So, if $a \not\equiv 0 \pmod p$, a is a dth power iff $a \equiv g^{kd} \pmod p$ for some k.

By example (Ex. 4.20), 2 is a primitive root modulo 19, so the 6th powers modulo 19 are $2^0 = 1, 2^6 = 7, 2^{12} = 11$. $\square$

Ex. 4.22 *If a has order 3 modulo p, show that $1+a$ has order 6.*

Proof. If a has order 3 modulo p, then $0 \equiv a^3 - 1 = (a-1)(a^2+a+1) \pmod p$, with $a \not\equiv 1 \pmod p$, so $a^2 + a + 1 \equiv 0 \pmod p$. Thus

$$\begin{aligned} (1+a)^3 &\equiv 1 + 3a + 3a^2 + a^3 \\ &\equiv 1 + 3a + 3(-1-a) + 1 \\ &\equiv -1 \pmod p \end{aligned}$$

So $(1+a)^6 \equiv 1 \pmod p$.

$(1+a)^2 \equiv 1 + 2a + a^2 = 1 + 2a + (-1-a) \equiv a \not\equiv 1 \pmod p$.

So $(1+a)^6 \equiv 1, (1+a)^2 \not\equiv 1, (1+a)^3 \not\equiv 1 \pmod p$, so the order of $1+a$ divides 6, but doesn't divides 2 or 3, so $1+a$ has order 6 modulo p. $\square$

Ex. 4.23 *Show that $x^2 \equiv -1 \pmod p$ has a solution iff $p \equiv 1 \pmod 4$, and that $x^4 \equiv -1 \pmod p$ has a solution iff $p \equiv 1 \pmod 8$.*

Proof. If $x^2 \equiv -1 \pmod p$, then $\overline{x}$ has order 4 in $\mathbb{F}_p^*$, hence from Lagrange's theorem, $4 \mid p-1$.

Reciprocally, suppose $4 \mid p-1$, so $p = 4k+1, k \in \mathbb{N}^*$. From proposition 4.2.1, as $2 \mid p-1$, -1 is a square modulo p iff $(-1)^{(p-1)/2} \equiv 1 \pmod p$, which is true because $(-1)^{(p-1)/2} = (-1)^{2k} = 1$.

If $x^4 \equiv -1 \pmod p$, then $\overline{x}^8 = 1 \in \mathbb{F}_p^*$, and $\overline{x}^4 \neq 1$, so x has order 8 in $\mathbb{F}_p^*$, so $8 \mid p-1$.

Reciprocally, if $p \equiv 1 \pmod 8$, $p = 8K+1, K \in \mathbb{N}^*$. From Prop.4.2.1, as $4 \mid p-1$, there exists $x \in \mathbb{Z}$ such that $-1 = x^4$ iff $(-1)^{(p-1)/4} \equiv 1 \pmod 8$, which is true because $(-1)^{(p-1)/4} = (-1)^{2K} = 1$.

Conclusion :

$$\exists x \in \mathbb{Z},\ x^4 \equiv -1 \pmod p \iff p \equiv 1 \pmod 8.$$

$\square$

Ex. 4.24 *Show that* $ax^m + by^n \equiv c \pmod p$ *has the same number of solutions as* $ax^{m'} + by^{n'} \equiv c \pmod p$*, where* $m' = (m, p-1)$ *and* $n' = (n, p-1)$*.*

Proof. If $a \wedge b \nmid c$, the two equations have no solution. So we can suppose $a \wedge b \mid c$, and after division by $\delta = a \wedge b$, we obtain an equation $a'x^m + b'y^n = c'$, $a' = a/\delta, b' = b\delta, c' = c\delta$, and $a' \wedge b' = 1$. So it remains to prove that $ax^m + by^n \equiv c \pmod p$ has the same number of solutions as $ax^{m'} + by^{n'} \equiv c \pmod p$ when $a \wedge b = 1$.

In this case the equation $au + bv = c$ has solutions. Let N the number of solutions $(\overline{x}, \overline{y})$ of the equation $\overline{a}\,\overline{x}^m + \overline{b}\,\overline{y}^n = \overline{c}$,$N'$ the number of solutions $(\overline{x}, \overline{y})$ of the equation $\overline{a}\,\overline{x}^{m'} + \overline{b}\,\overline{y}^{n'} = \overline{c}$. Then

$$\begin{aligned}
N &= \mathrm{Card}\{(\overline{x}, \overline{y}) \in \mathbb{F}_p \times \mathbb{F}_p \mid \overline{a}\,\overline{x}^m + \overline{b}\,\overline{y}^n = \overline{c}\} \\
&= \sum_{\overline{a}\overline{u} + \overline{b}\overline{v} = \overline{c}} \mathrm{Card}\{(\overline{x}, \overline{y}) \in \mathbb{F}_p \times \mathbb{F}_p \mid \overline{x}^m = \overline{u}, \overline{y}^n = \overline{v}\} \\
&= \sum_{\overline{a}\overline{u} + \overline{b}\overline{v} = \overline{c}} \mathrm{Card}\{\overline{x} \in \mathbb{F}_p \mid \overline{x}^m = \overline{u}\} \times \mathrm{Card}\{\overline{y} \in \mathbb{F}_p \mid \overline{y}^n = \overline{v}\}.
\end{aligned}$$

The same is true for N', so it is suffisant to prove that

$$\mathrm{Card}\{\overline{x} \in \mathbb{F}_p \mid \overline{x}^m = \overline{u}\} = \mathrm{Card}\{\overline{x} \in \mathbb{F}_p \mid \overline{x}^{m'} = \overline{u}\},$$

where $m' = m \wedge (p-1)$, and a similar equality for the equation $\overline{y}^n = \overline{v}$.

Let $\overline{g}$ a generator of $\mathbb{F}_p^*$. Write $\overline{u} = \overline{g}^r, r \in \mathbb{N}$.

$$\begin{aligned}
\exists \overline{x} \in \mathbb{F}_p,\ \overline{x}^m = \overline{u} &\iff \exists k \in \mathbb{Z},\ \overline{g}^{mk} = \overline{g}^r \\
&\iff \exists k \in \mathbb{Z},\ p-1 \mid mk - r \\
&\iff \exists k \in \mathbb{Z}, \exists l \in \mathbb{Z},\ r = mk + l(p-1) \\
&\iff m \wedge (p-1) \mid r
\end{aligned}$$

So

$$\{\overline{x} \in \mathbb{F}_p \mid \overline{x}^m = \overline{u}\} \neq \emptyset \iff m \wedge (p-1) \mid r,$$

and similarly

$$\{\overline{x} \in \mathbb{F}_p \mid \overline{x}^{m'} = \overline{u}\} \neq \emptyset \iff m' \wedge (p-1) \mid r.$$

Since $m' \wedge (p-1) = (m \wedge (p-1)) \wedge (p-1) = m \wedge (p-1)$, these two conditions are equivalent, so these two sets are empty for the same values of $\overline{u}$.

Let $\overline{u}$ is such that $\{\overline{x} \in \mathbb{F}_p \mid \overline{x}^m = \overline{u}\} \neq \emptyset$, and x_0 a fixed solution of $\overline{x}^m = \overline{u}$.

Write $\overline{x} = \overline{g}^k, \overline{x_0} = g^{k_0}$. Let $d = m \wedge (p-1) (= m')$.

$$\begin{aligned}
\overline{x}^m = u &\iff \overline{x}^m = \overline{x_0}^m \\
&\iff \overline{g}^{mk} = \overline{g}^{mk_0} \\
&\iff p-1 \mid m(k-k_0) \\
&\iff \frac{p-1}{d} \mid \frac{m}{d}(k-k_0) \\
&\iff \frac{p-1}{d} \mid k - k_0 \\
&\iff \exists j \in \mathbb{Z}, k = k_0 + j\frac{p-1}{d}
\end{aligned}$$

As g is a primitive root modulo p, the distinct solutions are $x_0, x_0 g^{\frac{p-1}{d}}, \ldots, x_0 g^{k\frac{p-1}{d}}, \ldots x_0 g^{(d-1)\frac{p-1}{d}}$, so in this case

$$\mathrm{Card}\{\overline{x} \in \mathbb{F}_p \mid \overline{x}^m = \overline{u}\} = d = m \wedge (p-1).$$

As $m' \wedge (p-1) = m \wedge (p-1)$,

$$\mathrm{Card}\{\overline{x} \in \mathbb{F}_p \mid \overline{x}^m = \overline{u}\} = \mathrm{Card}\{\overline{x} \in \mathbb{F}_p \mid \overline{x}^{m'} = \overline{u}\}.$$

So $N = N'$: $ax^m + by^n \equiv c \pmod p$ has the same number of solutions as $ax^{m'} + by^{n'} \equiv c \pmod p$, where $m' = (m, p-1)$ and $n' = (n, p-1)$. $\square$

Ex. 4.25 *Prove Propositions 4.2.2 and 4.2.4.*

Proposition 4.2.2. *Suppose that a is odd, $e \geq 3$, and consider the congruence $x^n \equiv a \pmod{2^e}$. If n is odd, a solution always exists and it is unique.*

If n is even, a solution exists iff $a \equiv 1 \pmod 4, a^{2^{e-2}/d} \equiv 1 \pmod{2^e}$, where $d = (n, 2^{e-2})$. When a solution exists there are exactly $2d$ solutions.

Proof. We suppose that a is odd and $e \geq 3$.

From Theorem 2', we know that $\{(-1)^a 5^b \mid 0 \leq a \leq 1, 0 \leq b \leq 2^{e-2}\}$ constitutes a reduced residue system modulo 2^e, so we can write

$$\begin{aligned} a &\equiv (-1)^s 5^t \pmod{2^e}, 0 \leq s \leq 1, 0 \leq t \leq 2^{e-2}, \\ x &\equiv (-1)^y 5^z \pmod{2^e}, 0 \leq y \leq 1, 0 \leq z \leq 2^{e-2}. \end{aligned}$$

For all $x \in \mathbb{Z}$,

$$x^n \equiv a \pmod{2^e} \iff (-1)^{ny} 5^{nz} \equiv (-1)^s 5^t \pmod{2^e}$$

Then $(-1)^{ny} \equiv (-1)^s \pmod 4, ny \equiv s \pmod 2, (-1)^{ny} = (-1)^s$, so $5^{nz} \equiv 5^t \pmod{2^e}$.

Reciprocally, if $ny \equiv s \pmod 2$ and $5^{nz} \equiv 5^t \pmod{2^e}$, then $x^n \equiv a \pmod{2^e}$, so

$$x^n \equiv a \pmod{2^e} \iff \left\{ \begin{array}{lll} ny & \equiv & s \pmod 2 \\ 5^{nz} & \equiv & 5^t \pmod{2^e} \end{array} \right. \iff \left\{ \begin{array}{lll} ny & \equiv & s \pmod 2 \\ nz & \equiv & t \pmod{2^{e-2}} \end{array} \right.$$

since the order of 5 modulo 2^e is 2^{e-2}.

• Suppose that n is an odd integer. Then

$$\left\{ \begin{array}{lll} ny & \equiv & s \pmod 2 \\ nz & \equiv & t \pmod{2^{e-2}} \end{array} \right. \iff \left\{ \begin{array}{lll} y & \equiv & s \pmod 2 \\ z & \equiv & n't \pmod{2^{e-2}} \end{array} \right.$$

where n' is an inverse of n modulo 2^{e-2} : $nn' \equiv 1 \pmod{2^{e-2}}$.

So $x^n \equiv a \pmod{2^e}$ has an unique solution modulo 2^e.

• Suppose that n is an even integer.

Then $\left\{ \begin{array}{lll} ny & \equiv & s \pmod 2 \\ nz & \equiv & t \pmod{2^{e-2}} \end{array} \right.$ implies $s \equiv 0 \pmod 2$ and $d = n \wedge 2^{e-2} \mid t$.

Then $a \equiv (-1)^s 5^t \equiv 5^t \pmod{2^e}$, so $a \equiv 1 \pmod 4$.

Hence $a^{\frac{2^{e-2}}{d}} \equiv \left(5^{2^{e-2}}\right)^{\frac{t}{d}} \equiv 1 \pmod{2^e}$, since 5 has order 2^{e-2}, and $d \mid t$.

So, if n is even, and $d = n \wedge 2^{e-2}$,

$$\exists x \in \mathbb{Z},\ x^n \equiv a \pmod{2^e} \Rightarrow \left\{ \begin{array}{lll} a & \equiv & 1 \pmod 4 \\ a^{\frac{2^{e-2}}{d}} & \equiv & 1 \pmod{2^e} \end{array} \right.$$

Reciprocally, suppose that $\left\{\begin{array}{lcl} a & \equiv & 1 \pmod 4 \\ a^{\frac{2^{e-2}}{d}} & \equiv & 1 \pmod{2^e} \end{array}\right.$. Then $a \equiv (-1)^s 5^t \pmod{2^e}$ implies $a \equiv (-1)^s \pmod 4$, so s is even, and $a \equiv 5^t \pmod{2^e}$.

Therefore $5^{t\frac{2^{e-2}}{d}} \equiv 1 \pmod{2^e}$, which implies $2^{e-2} \mid t\frac{2^{e-2}}{d}$, so $d \mid t$.

$$\begin{aligned}
\exists x \in \mathbb{Z},\ x^n \equiv a \pmod{2^e} &\iff \exists y \in \mathbb{Z},\ \exists z \in \mathbb{Z},\ \left\{\begin{array}{lcll} ny & \equiv & s & \pmod 2 \\ nz & \equiv & t & \pmod{2^{e-2}} \end{array}\right. \\
&\iff \exists z \in \mathbb{Z},\ nz \equiv t \pmod{2^{e-2}} \qquad (\text{since } n, s \text{ even}) \\
&\iff \exists z \in \mathbb{Z},\ 2^{e-2} \mid nz - t \\
&\iff \exists z \in \mathbb{Z},\ \frac{2^{e-2}}{d} \mid \frac{n}{d}z - \frac{t}{d} \\
&\iff \exists z \in \mathbb{Z},\ \exists q \in \mathbb{Z},\ q\frac{2^{e-2}}{d} + z\frac{n}{d} = \frac{t}{d}
\end{aligned}$$

As $\frac{2^{e-2}}{d} \wedge \frac{n}{d} = 1$, there exists a solution (q, z_0) of this last equation, where $0 \le z_0 < \frac{2^{e-2}}{d}$, and so $x_0 = 5^{z_0}$ is a particular solution of $x^n \equiv a \pmod{2^e}$, therefore

$$\exists x \in \mathbb{Z},\ x^n \equiv a \pmod{2^e} \iff \left\{\begin{array}{lcll} a & \equiv & 1 & \pmod 4 \\ a^{\frac{2^{e-2}}{d}} & \equiv & 1 & \pmod{2^e} \end{array}\right.$$

If there exists a particular solution $x_0 \equiv (-1)^{y_0} 5^{z_0}$, then

$$\begin{aligned}
x^n \equiv a \pmod{2^e} &\iff x^n \equiv x_0^n \pmod{2^e} \\
&\iff \left\{\begin{array}{lcll} ny & \equiv & ny_0 & \pmod 2 \\ nz & \equiv & nz_0 & \pmod{2^{e-2}} \end{array}\right. \\
&\iff n(z - z_0) \equiv 0 \pmod{2^{e-2}} \qquad (\text{since } n \text{ even}) \\
&\iff \frac{2^{e-2}}{d} \mid \frac{n}{d}(z - z_0) \\
&\iff \frac{2^{e-2}}{d} \mid z - z_0, \qquad \left(\text{since } \frac{2^{e-2}}{d} \wedge \frac{n}{d} = 1\right) \\
&\iff \exists k \in \mathbb{Z},\ z = z_0 + k\frac{2^{e-2}}{d}
\end{aligned}$$

As the order of 5 modulo 2^e is 2^{e-2}, the solutions of $x^n \equiv a \pmod{2^e}$ are

$$x_k = (-1)^y 5^{z_0 + k\frac{2^{e-2}}{d}},\ 0 \le y < 2,\ 0 \le k < d,$$

so there are exactly $2d$ solutions modulo 2^e. □

Proposition 4.2.4. *Let 2^l be the highest power of 2 dividing n. Suppose that a is odd and that $x^n \equiv a \pmod{2^{2l+1}}$ is solvable. Then $x^n \equiv a \pmod{2^e}$ is solvable for all $e \ge 2l+1$, and consequently for all $e \ge 1$). Moreover, all these congruences have the same number of solutions.*

Proof. We suppose that a is odd, and that $x^n \equiv a \pmod{2^{2l+1}}$ is solvable. l is such that $n = 2^l n'$, where n' is an odd integer.

Let the induction hypothesis be, for a fixed integer $m \ge 2l+1$,

$$\exists x_0 \in \mathbb{Z},\ x_0^n \equiv a \pmod{2^m}.$$

Let $x_1 = x_0 + b2^{m-l}$: we show that for an appropriate choice of $b \in \{0,1\}$, $x_1^n \equiv a \pmod{2^{m+1}}$.

$x_1^n = x_0^n + nb2^{m-l}x_0^{n-1} + 2^{2m-2l}A,\ A \in \mathbb{Z}$.

Since $m \geq 2l+1, 2m-2l \geq m+1$, so

$$x_1^n \equiv x_0^n + nb2^{m-l}x_0^{n-1} \pmod{2^{m+1}}.$$

$$\begin{aligned} x_1^n \equiv a \pmod{2^{m+1}} &\iff (x_0^n - a) + n'bx_0^{n-1}2^m \equiv 0 \pmod{2^{n+1}} \\ &\iff \frac{x_0^n - a}{2^m} + n'bx_0^{n-1} \equiv 0 \pmod{2} \end{aligned}$$

As a is odd, and $x_0^n \equiv a \pmod{2^m}, m \geq 1$, x_0 is odd, and n' is odd, so there exists an unique $b \in \{0,1\}$ such that $\frac{x_0^n - a}{2^m} + n'bx_0^{n-1} \equiv 0 \pmod{2}$. So there exists $x_1 \in \mathbb{Z}$ such that $x_1^b \equiv a \pmod{2^{m+1}}$, and the induction is completed. Therefore, $x^n \equiv a \pmod{2^e}$ is solvable for all $e \geq 2l+1$, and consequently for all $e \geq 1$).

From the Proposition 4.2.2., with the hypothesis $e \geq 3$, we know that the number of solutions of the solvable equation $x^n \equiv a \pmod{2^e}, e \geq 2l+1$, is 1 if n is odd, $2(n \wedge 2^{e-2})$ if n is even.

If n is even, $l \geq 1$, $e \geq 2l+1 \geq 3$. Since $e \geq 2l+1$, and $n = 2^l n'$ for an odd n', $l \leq \frac{e-1}{2} \leq e-2$, so $n \wedge 2^{e-2} = n'2^l \wedge 2^{e-2} = 2^l$, and the number of solutions is 2^{l+1}, independent of $e \geq 2l+1$.

Conclusion : under the hypothesis $x^n \equiv a \pmod{2^{2l+1}}$, where $l = \mathrm{ord}_2(n)$, then $x^n \equiv a \pmod{2^e}$ is solvable for all $e \geq 1$, and all these congruences have the same number of solutions for $e \geq 2l+1, e \geq 3$. □

Chapter 5

Ex. 5.1 *Use Gauss' lemma to determine* $\left(\frac{5}{7}\right), \left(\frac{3}{11}\right), \left(\frac{6}{13}\right), \left(\frac{-1}{p}\right)$.

Proof. • $a = 5, p = 7$.

The array of values of the least residues modulo $p = 7$, for $1 \leq k \leq (p-1)/2$.

$k \mod 7$	1	2	3
$5k \mod 7$	-2	3	1

So the number of negative least residues is $\mu = 1$, and $\left(\frac{5}{7}\right) = (-1)^\mu = -1$.

• $a = 3, p = 11$.

$k \mod 11$	1	2	3	4	5
$3k \mod 11$	3	-5	-2	1	4

So $\mu = 2$, $\left(\frac{3}{11}\right) = (-1)^\mu = 1$.

• $a = 6, p = 13$.

$k \mod 13$	1	2	3	4	5	6
$6k \mod 13$	6	-1	5	-2	4	-3

So $\mu = 3$, $\left(\frac{6}{13}\right) = (-1)^\mu = -1$.

• If $a = -1$, and p an odd prime, the values of the least residues of $-k$ modulo p for $k = 1, 2, \ldots, (p-1)/2$ are $-k$, all negative. So the number of negative least residues is $\mu = (p-1)/2$, and $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. □

Ex. 5.2 *Show that the number of solutions to* $x^2 \equiv a \pmod p$ *is equal to* $1 + (a/p)$.

Proof. Let N the number of solutions of $x^2 \equiv a \pmod p$.

• If $\left(\frac{a}{p}\right) = 0$, then $p \mid a$, $a \equiv 0 \pmod p$, so the unique solution of $x^2 \equiv a = 0$ is $x \equiv 0 \pmod p$, so $N = 1 = 1 + \left(\frac{a}{p}\right)$.

• If $\left(\frac{a}{p}\right) = -1$, then $N = 0 = 1 + \left(\frac{a}{p}\right)$.

• If $\left(\frac{a}{p}\right) = 1$, then $x^2 \equiv a \pmod p$ has a solution x_0, and $x^2 \equiv a \pmod p \iff x^2 \equiv x_0^2 \pmod p \equiv p \mid (x - x_0)(x + x_0) \equiv x \equiv \pm x_0 \pmod p$, so $N = 2 = 1 + \left(\frac{a}{p}\right)$. ☐