1. The Unit Group of $\mathbb{Z}/n\mathbb{Z}$

Consider a nonunit positive integer,
\[ n = \prod p^e_r > 1. \]

The Sun Ze Theorem gives a ring isomorphism,
\[ \mathbb{Z}/n\mathbb{Z} \cong \prod \mathbb{Z}/p^e_r\mathbb{Z}. \]

The right side is the cartesian product of the rings $\mathbb{Z}/p^e_r\mathbb{Z}$, meaning that addition and multiplication are carried out componentwise. It follows that the corresponding unit group is
\[ (\mathbb{Z}/n\mathbb{Z})^\times \cong \prod (\mathbb{Z}/p^e_r\mathbb{Z})^\times. \]

Thus to study the unit group $(\mathbb{Z}/n\mathbb{Z})^\times$ it suffices to consider $(\mathbb{Z}/p^e\mathbb{Z})^\times$ where $p$ is prime and $e > 0$. Recall that in general,
\[ |(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n), \]
so that for prime powers,
\[ |(\mathbb{Z}/p^e\mathbb{Z})^\times| = \phi(p^e) = p^{e-1}(p - 1), \]
and especially for primes,
\[ |(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1. \]

Here are some examples of unit groups modulo prime powers, most but not quite all cyclic.

- $(\mathbb{Z}/2\mathbb{Z})^\times = \{\{1\}, \cdot\} = \{\{2^0\}, \cdot\} \cong \{\{0\}, \cdot\} = \mathbb{Z}/2\mathbb{Z}$,
- $(\mathbb{Z}/3\mathbb{Z})^\times = \{\{1, 2\}, \cdot\} = \{\{2^0, 2^1\}, \cdot\} \cong \{\{0, 1\}, \cdot\} = \mathbb{Z}/2\mathbb{Z}$,
- $(\mathbb{Z}/4\mathbb{Z})^\times = \{\{1, 3\}, \cdot\} = \{\{3^0, 3^1\}, \cdot\} \cong \{\{0, 1\}, \cdot\} = \mathbb{Z}/2\mathbb{Z}$,
- $(\mathbb{Z}/5\mathbb{Z})^\times = \{\{1, 2, 3, 4, \cdot\} = \{\{2^0, 2^1, 2^2, 2^3, \cdot\} \cong \{\{0, 1, 2, 3, \cdot\} = \mathbb{Z}/4\mathbb{Z}$,
- $(\mathbb{Z}/7\mathbb{Z})^\times = \{\{1, 2, 3, 4, 5, 6\}, \cdot\} = \{\{3^0, 3^1, 3^2, 3^3, 3^4, 3^5\}, \cdot\}
  \cong \{\{0, 1, 2, 3, 4, 5\}, \cdot\} = \mathbb{Z}/6\mathbb{Z}$,
- $(\mathbb{Z}/8\mathbb{Z})^\times = \{\{1, 3, 5, 7\}, \cdot\} = \{\{3^0, 3^3, 3^5\}, \cdot\}
  \cong \{\{0, 1\} \times \{0, 1\}, \cdot\} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$,
- $(\mathbb{Z}/9\mathbb{Z})^\times = \{\{1, 2, 4, 5, 7, 8\}, \cdot\} = \{\{2^0, 2^1, 2^2, 2^3, 2^4, 2^5\}, \cdot\}
  \cong \{\{0, 1, 2, 3, 4, 5\}, \cdot\} = \mathbb{Z}/6\mathbb{Z}$.
2. Prime Unit Group Structure: Abelian Group Theory Argument

**Proposition 2.1.** Let $G$ be any finite subgroup of the unit group of any field. Then $G$ is cyclic. In particular, the multiplicative group modulo any prime $p$ is cyclic, \((\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p - 1)\mathbb{Z}\).

That is, there is a generator $g$ mod $p$ such that \((\mathbb{Z}/p\mathbb{Z})^\times = \{1, g, g^2, \ldots, g^{p-2}\}\).

**Proof.** We may assume that $G$ is not trivial. By the structure theorem for finitely generated abelian groups, 
\((G, \cdot) \cong (\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}, +),\quad k \geq 1, 1 < d_1 \mid d_2 \cdots \mid d_k.

Thus the polynomial equation $X^{d_k} = 1$, whose additive counterpart is $d_kX = 0$, is satisfied by each of the $d_1d_2\cdots d_k$ elements of $G$; but also, the polynomial has at most as many roots as its degree $d_k$. Thus $k = 1$ and $G$ is cyclic. \(\square\)

The proof tacitly relies on a fact from basic algebra:

**Lemma 2.2.** Let $k$ be a field. Let $f \in k[X]$ be a nonzero polynomial, and let $d$ denote its degree (thus $d \geq 0$). Then $f$ has at most $d$ roots in $k$.

**Proof.** If $f$ has no roots then we are done. Otherwise let $a \in k$ be a root. Write
\[ f(X) = q(X)(X - a) + r(X), \quad \text{deg}(r) < 1 \text{ or } r = 0. \]

Thus $r(X)$ is a constant. Substitute $a$ for $X$ to see that in fact $r = 0$, and so $f(X) = q(X)(X - a)$. By induction, $q$ has at most $d - 1$ roots in $k$ and we are done. \(\square\)

The lemma does require that $k$ be a field, not merely a ring. For example, the polynomial $X^2 - 1$ over the ring $\mathbb{Z}/24\mathbb{Z}$ has for its roots
\[ \{1, 5, 7, 11, 13, 17, 19, 23\} = (\mathbb{Z}/24\mathbb{Z})^\times. \]

To count the generators of $(\mathbb{Z}/p\mathbb{Z})^\times$, we establish a handy result that is slightly more general.

**Proposition 2.3.** Let $n$ be a positive integer, and let $e$ be an integer. The map \[ \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \quad x \mapsto ex \]
has

image $\langle \gcd(e, n) + n\mathbb{Z} \rangle$, of order $n/\gcd(e, n)$,

kernel $\langle n/\gcd(e, n) + n\mathbb{Z} \rangle$, of order $\gcd(e, n)$.

Indeed, the image is $\{ex + n\mathbb{Z} : x \in \mathbb{Z}\} = \{ex + ny + n\mathbb{Z} : x, y \in \mathbb{Z}\} = \langle \gcd(e, n) + n\mathbb{Z} \rangle$, and the rest of the proposition follows.

Especially, each $e + n\mathbb{Z}$ where $e$ is coprime to $n$ generates the full group, and there are $\phi(n)$ such values of $e$.

Because $(\mathbb{Z}/p\mathbb{Z})^\times$ is isomorphic to $\mathbb{Z}/(p - 1)\mathbb{Z}$, the proposition shows that if $g$ is a generator then the other generators are precisely the powers $g^e$ where $\gcd(e, p - 1) = 1$. Thus there are $\phi(p - 1)$ generators altogether.
3. **Prime Unit Group Structure: Elementary Argument**

From above, a nonzero polynomial over \( \mathbb{Z}/p\mathbb{Z} \) cannot have more roots than its degree. On the other hand, Fermat’s Little Theorem says that the polynomial

\[
f(X) = X^{p-1} - 1 \in (\mathbb{Z}/p\mathbb{Z})[X]
\]

has a full contingent of \( p - 1 \) roots in \( \mathbb{Z}/p\mathbb{Z} \).

For any divisor \( d \) of \( p - 1 \), consider the factorization (in consequence of the finite geometric sum formula)

\[
f(X) = X^{p-1} - 1 = (X^d - 1) \sum_{i=0}^{p-1-d} X^{id} \equiv g(X)h(X).
\]

We know that

- \( f \) has \( p - 1 \) roots in \( \mathbb{Z}/p\mathbb{Z} \),
- \( g \) has at most \( d \) roots in \( \mathbb{Z}/p\mathbb{Z} \),
- \( h \) has at most \( p - 1 - d \) roots in \( \mathbb{Z}/p\mathbb{Z} \).

It follows that \( g(X) = X^d - 1 \) where \( d \mid p - 1 \) has \( d \) roots in \( \mathbb{Z}/p\mathbb{Z} \).

Now factor \( p - 1 \),

\[
p - 1 = \prod q^e.
\]

For each factor \( q^e \) of \( p - 1 \),

\[
X^{q^e} - 1 \quad \text{has } q^e \text{ roots in } \mathbb{Z}/p\mathbb{Z},
\]

\[
X^{q^e-1} - 1 \quad \text{has } q^{e-1} \text{ roots in } \mathbb{Z}/p\mathbb{Z},
\]

and so \( (\mathbb{Z}/p\mathbb{Z})^\times \) contains \( q^e - q^{e-1} = \phi(q^e) \) elements \( x_q \) of order \( q^e \). (The order of an element is the smallest positive number of times that the element is multiplied by itself to give 1.) Plausibly,

\[
\text{any product } \prod x_q \text{ has order } \prod q^e = p - 1,
\]

and certainly there are \( \phi(p - 1) \) such products. In sum, we have done most of the work of showing

**Proposition 3.1.** Let \( p \) be prime. Then \( (\mathbb{Z}/p\mathbb{Z})^\times \) is cyclic, with \( \phi(p-1) \) generators.

The loose end is as follows.

**Lemma 3.2.** In a commutative group, consider two elements whose orders are coprime. Then the order of their product is the product of their orders.

**Proof.** We have \( a^e = b^f = 1 \), and so

\[
(ab)^{ef} = (a^e)^f (b^f)^e = 1^f 1^e = 1.
\]

Also we have \( (e, f) = 1 \). So for any positive integer \( d \),

\[
(ab)^d = 1 \implies 1 = ((ab)^d)^e = (a^e b^e)^d = b^{ed} \implies f \mid cd \implies f \mid d,
\]

and symmetrically \( e \mid d \). Thus \( ef \mid d \). \( \square \)
4. Odd Prime Power Unit Group Structure: $p$-Adic Argument

**Proposition 4.1.** Let $p$ be an odd prime, and let $e$ be any positive integer. The multiplicative group modulo $p^e$ is cyclic.

**Proof.** (Sketch.) We have the result for $e = 1$, so take $e \geq 2$. The structure theorem for finitely generated abelian groups and then the Sun Ze theorem combine to show that $(\mathbb{Z}/p^e\mathbb{Z})^\times$ takes the form

$$(\mathbb{Z}/p^e\mathbb{Z})^\times = A_{p^e-1} \times A_{p-1}$$

(where $A_n$ denotes an abelian group of order $n$).

By the Sun Ze Theorem, it suffices to show that each of $A_{p^e-1}$ and $A_{p-1}$ is cyclic.

The natural epimorphism $\mathbb{Z}/p^e\mathbb{Z} \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ maps $A_{p^e-} to 1$ in $(\mathbb{Z}/p\mathbb{Z})^\times$ since the orders of the two groups are coprime but the image is a quotient of the first and a subgroup of the second. Consequently the restriction of the natural epimorphism to $A_{p-1}$ must be an isomorphism, and thus $A_{p-1}$ is cyclic because $(\mathbb{Z}/p\mathbb{Z})^\times$ is. Furthermore, this discussion has shown that $A_{p^e-1}$ is the kernel of the natural epimorphism,

$A_{p^e-1} = \{a + p^e\mathbb{Z} : a = 1 \mod p\}$.

Working $p$-adically, consider the group isomorphism

$$\exp : p\mathbb{Z}_p \rightarrow 1 + p\mathbb{Z}_p.$$ 

The exponential series converges on $p\mathbb{Z}_p$ because the summands decay notwithstanding the factorial in the denominator,

$$\nu_p\left(\frac{(ap)^n}{n!}\right) = n - \sum_{i \geq 1} \frac{n}{p^i} = n\left(1 - \frac{1}{p^i}\right) \geq \frac{n}{2}, \quad n \in \mathbb{Z}_{\geq 0}.$$ 

Similarly, the exponential map takes $p^e\mathbb{Z}_p$ into $1 + p^e\mathbb{Z}_p$ for any $e \geq 1$, as follows. The first two terms of $\exp(ap^e)$ for any $a \in \mathbb{Z}_p$ are $1 + ap^e$, and then for $n \geq 2$,

$$\nu_p\left(\frac{(ap^e)^n}{n!}\right) = n\left(e - \frac{1}{p^i}\right) \geq 2\left(e - \frac{1}{2}\right) = 2e - 1 \geq e.$$

Now we know that the surjective composition $p\mathbb{Z}_p \xrightarrow{\exp} 1 + p\mathbb{Z}_p \rightarrow A_{p^e-1}$, where the second map is the restriction of the ring map $\mathbb{Z}_p \rightarrow \mathbb{Z}_p/p^e\mathbb{Z}_p \approx \mathbb{Z}/p^e\mathbb{Z}$ to the multiplicative subgroup $1 + p\mathbb{Z}_p$ of $\mathbb{Z}_p$, factors through the quotient $p\mathbb{Z}_p/p^e\mathbb{Z}_p \approx \mathbb{Z}/p^e\mathbb{Z} \approx (\mathbb{Z}/p\mathbb{Z})^\times$. The resulting surjection $p\mathbb{Z}_p/p^e\mathbb{Z}_p \rightarrow A_{p^e-1}$ is an isomorphism because the two finite groups have the same order,

$$\begin{array}{ccc}
p\mathbb{Z}_p & \xrightarrow{\sim} & 1 + p\mathbb{Z}_p \\
\exp & & \\
p\mathbb{Z}_p/p^e\mathbb{Z}_p & \xrightarrow{\sim} & A_{p^e-1}
\end{array}$$

Because $p\mathbb{Z}_p/p^e\mathbb{Z}_p$ is cyclic, so is $A_{p^e-1}$, and the proof is complete. \qed

The condition $1 - 1/(p-1) > 0$ in the proof fails for $p = 2$, but a modification of the argument shows that $(\mathbb{Z}/2^e\mathbb{Z})^\times$ has a cyclic subgroup of index 2.

Once one is aware that the truncated exponential series gives an isomorphism $p\mathbb{Z}/p^e\mathbb{Z} \xrightarrow{\sim} A_{p^e-1}$, the isomorphism can be confirmed without direct reference to the $p$-adic exponential. For example with $e = 3$, any $px + p^3\mathbb{Z}$ has image $1 + px + \frac{1}{2}p^2x^2 + p^3\mathbb{Z}$, and similarly $py + p^3\mathbb{Z}$ has image $1 + py + \frac{1}{2}p^2y^2 + p^3\mathbb{Z}$; their
sum \( p(x + y) + p^3 \mathbb{Z} \) maps to \( 1 + p(x + y) + \frac{1}{2} p^2 (x^2 + 2xy + y^2) + p^3 \mathbb{Z} \), which is also the product of the images, even though \( 1 + p(x + y) + \frac{1}{2} p^2 (x^2 + 2xy + y^2) \) is not the product of \( 1 + px + \frac{1}{2} p^2 x^2 \) and \( 1 + py + \frac{1}{2} p^2 y^2 \). This idea underlies the elementary argument to be given next.

5. ODD PRIME POWER UNIT GROUP STRUCTURE: ELEMENTARY ARGUMENT

Again we show that for any odd prime \( p \) and any positive \( c \), the group \( (\mathbb{Z}/p^c \mathbb{Z})^\times \) is cyclic. Here the argument is elementary.

Proof. Let \( g \) generate \( (\mathbb{Z}/p^c \mathbb{Z})^\times \). Since

\[
(g + p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p \mod p^2 \neq g^{p-1} \mod p^2,
\]

it follows that

\[ g^{p-1} \not\equiv 1 \mod p^2 \quad \text{or} \quad (g + p)^{p-1} \not\equiv 1 \mod p^2. \]

So after replacing \( g \) with \( g + p \) if necessary, we may assume that \( g^{p-1} \not\equiv 1 \mod p^2 \).

Thus we know that

\[ g^{p-1} = 1 + k_1 p, \quad p \nmid k_1. \]

By the Binomial Theorem,

\[
g^{p(p-1)} = (1 + k_1 p)^p = 1 + pk_1 p + \sum_{j=2}^{p-1} \binom{p}{j} k_1^j p^j + k_1^p p^p
\]

\[ = 1 + k_2 p^2, \quad p \nmid k_2. \]

The last equality holds because the terms in the sum and the term \( k_1^p p^p \) are multiples of \( p^3 \). (Here it is relevant that \( p > 2 \). The assertion fails for \( p = 2 \), \( g = 3 \) because of the last term. That is, \( 3^2 - 1 = 1 + 1 \cdot 2 \) so that \( k_1 = 1 \) is not divisible by \( p = 2 \), but then \( 3^{2(2-1)} = 9 = 1 + 2 \cdot 2^2 \) so that \( k_2 = 2 \) is.) Again by the Binomial Theorem,

\[
g^{p^2(p-1)} = (1 + k_2 p^2)^p = 1 + pk_2 p^2 + \sum_{j=2}^{p} \binom{p}{j} k_2^j p^{2j}
\]

\[ = 1 + k_3 p^3, \quad p \nmid k_3, \]

because the terms in the sum are multiples of \( p^4 \). Similarly

\[
g^{p^3(p-1)} = 1 + k_4 p^4, \quad p \nmid k_4,
\]

and so on, up to

\[
g^{p^{c-2}(p-1)} = 1 + k_{c-1} p^{c-1}, \quad p \nmid k_{c-1}.
\]

That is,

\[
g^{p^{c-2}(p-1)} \not\equiv 1 \mod p^c.
\]

The order of \( g \) in \( (\mathbb{Z}/p^c \mathbb{Z})^\times \) must divide \( \phi(p^c) = p^{c-1}(p - 1) \). If the order takes the form \( p^e d \) where \( e \leq c - 1 \) and \( d \) is a proper divisor of \( p - 1 \) then Fermat’s Little Theorem \( (g^p = g \mod p) \) shows that the relation

\[
g^{p^e d} = 1 \mod p^e
\]

reduces modulo \( p \) to

\[ g^d = 1 \mod p. \]
But this contradicts the fact that \( g \) is a generator modulo \( p \). Thus the order of \( g \) in \( (\mathbb{Z}/p^e\mathbb{Z})^\times \) takes the form \( p^e(r-1) \) where \( e \leq e - 1 \). The calculation above has shown that \( e = e - 1 \), and the proof is complete. \( \square \)

For example, \( 2 \) generates \( (\mathbb{Z}/5\mathbb{Z})^\times \), and \( 2^{5-1} = 16 \neq 1 \mod 5^2 \), so in fact \( 2 \) generates \( (\mathbb{Z}/5^e\mathbb{Z})^\times \) for all \( e \geq 1 \).

A small consequence of the proposition is that since \( (\mathbb{Z}/p^e\mathbb{Z})^\times \) is cyclic for odd \( p \), and since \( \phi(p^e) = p^{e-1}(p-1) \) is even, the equation

\[ x^2 = 1 \mod p^e \]

has two solutions: 1 and \( g^{\phi(p^e)/2} \).

6. POWERS OF 2 UNIT GROUP STRUCTURE

**Proposition 6.1.** The structure of the unit group \( (\mathbb{Z}/2^e\mathbb{Z})^\times \) is

\[
(\mathbb{Z}/2^e\mathbb{Z})^\times \cong \begin{cases} 
\mathbb{Z}/\mathbb{Z} & \text{if } e = 1, \\
\mathbb{Z}/2\mathbb{Z} & \text{if } e = 2, \\
(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{e-2}\mathbb{Z}) & \text{if } e \geq 3.
\end{cases}
\]

Specifically, \( (\mathbb{Z}/2\mathbb{Z})^\times = \{1\} \), \( (\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3\} \), and for \( e \geq 3 \),

\[
(\mathbb{Z}/2^e\mathbb{Z})^\times \cong \{\pm 1\} \times \{1, 5, 5^2, \ldots, 5^{e-2}-1\}.
\]

**Proof.** The results for \( (\mathbb{Z}/2\mathbb{Z})^\times \) and for \( (\mathbb{Z}/4\mathbb{Z})^\times \) are readily observable, and so we take \( e \geq 3 \).

Since \( |(\mathbb{Z}/2^e\mathbb{Z})^\times| = \phi(2^e) = 2^{e-1} \), we need to show that

\[ 5^{2^{e-1}} \neq 1 \mod 2^e, \quad 5^{2^{e-2}} = 1 \mod 2^e, \]

Similarly, to the previous argument, start from

\[ 5^{2^0} = 5 = 1 + k_2 2^2, \quad 2 \nmid k_2, \]

and thus

\[ 5^{2^1} = 5^2 = 1 + 2k_2 2^2 + k_2^2 2^4 = 1 + k_3 2^3, \quad 2 \nmid k_3, \]

and then

\[ 5^{2^2} = 5^4 = 1 + 2k_3 2^3 + k_3^2 2^6 = 1 + k_4 2^4, \quad 2 \nmid k_4, \]

and so on up to

\[ 5^{2^{e-3}} = 1 + k_{e-2} 2^{e-1}, \quad 2 \nmid k_{e-2}, \]

and finally

\[ 5^{2^{e-2}} = 1 + k_e 2^e, \quad 2 \nmid k_e. \]

The last two displays show that

\[ 5^{2^{e-3}} \neq 1 \mod 2^e, \quad 5^{2^{e-2}} = 1 \mod 2^e. \]

That is, 5 generates half of \( (\mathbb{Z}/2^e\mathbb{Z})^\times \). To show that the full group is

\[
(\mathbb{Z}/2^e\mathbb{Z})^\times \cong \{\pm 1\} \times \{1, 5, 5^2, \ldots, 5^{e-2}-1\},
\]

suppose that

\[
(-1)^a 5^b = (-1)^c 5^d \mod 2^e, \quad a, c \in \{0, 1\}, \quad b, d \in \{0, \ldots, 2^{e-2} - 1\}.
\]

Inspect modulo 4 to see that \( c = a \). So now \( 5^b = 5^d \mod 2^e \), and the restrictions on \( b \) and \( d \) show that \( d = b \) as well. \( \square \)
The group \((\mathbb{Z}/2^e\mathbb{Z})^\times\) is not cyclic for \(e \geq 3\) because all of its elements have order dividing \(2^{e-2}\).

The equation
\[
x^2 = 1 \mod 2^e
\]
has one solution if \(e = 1\), two solutions if \(e = 2\), and four solutions if \(e \geq 3\),

\((1, 1), \ (-1, 1), \ (1, 5^{2^{e-3}}), \ (-1, 5^{2^{e-3}})\).

With this information in hand, the Sun Ze Theorem shows that the number of solutions of the equation
\[
x^2 \equiv 1 \mod n,
\]
(where \(n = 2^e \prod_{i=1}^{g} p_i^{e_i}\)) is
\[
\begin{cases}
2^g & \text{if } e = 0, 1,
2 \cdot 2^g & \text{if } e = 2,
4 \cdot 2^g & \text{if } e \geq 3.
\end{cases}
\]

For example, if \(n = 120 = 2^3 \cdot 3 \cdot 5\) then the number of solutions is 16.

Especially, the fact that for odd \(n = \prod_{i=1}^{g} p_i^{e_i}\) there are \(2^g - 1\) proper square roots of 1 modulo \(n\) has to do with the effectiveness of the Miller–Rabin primality test. Recall that the test makes use of a diagnostic base \(b \in \{1, \ldots, n-1\}\) and of the factorization \(n - 1 = 2^s m\), computing (everything modulo \(n\))
\[
b^m, \ (b^m)^2, \ ((b^m)^2)^2, \ldots, \ (b^{m2^{e-2}})^2 = b^{n-1}.
\]

Of course, if \(b^m = 1\) then all the squaring is doing nothing, while if \(b^{n-1} \neq 1\) then \(n\) is not prime by Fermat’s Little Theorem. The interesting case is when \(b^m \neq 1\) but \(b^{n-1} = 1\), so that repeatedly squaring \(b^m\) does give 1: in this case, squaring \(b^m\) one fewer time gives a proper square root of 1. If \(n\) has \(g\) distinct prime factors then we expect this square root to be \(-1\) only \(1/(2^g - 1)\) of the time. Thus, if the process turns up the square root \(-1\) for many values of \(b\) then almost certainly \(g = 1\), i.e., \(n\) is a prime power. Of course, if \(n\) is a prime power but not prime then we hope that it isn’t a Fermat pseudoprime base \(b\) for many bases \(b\), and the Miller–Rabin will diagnose this.

7. Cyclic Unit Groups \((\mathbb{Z}/n\mathbb{Z})^\times\)

Consider a positive nonunit integer
\[
n = \prod_i p_i^{e_i}.
\]

Recall the multiplicative component of the Sun Ze Theorem,
\[
(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \prod \left(\mathbb{Z}/p_i^{e_i}\mathbb{Z}\right)^\times, \quad a \mod n \mapsto (a \mod p_i^{e_i}, \ldots, a \mod p_k^{e_k}).
\]

Consequently, the order of \(a\) divides the least common multiple of the orders of the multipicand-groups,
\[
lcm\{\phi(p_1^{e_1}), \ldots, \phi(p_k^{e_k})\},
\]
and thus \(a\) can not conceivably have order \(\phi(n)\) unless all of the \(\phi(p_i^{e_i})\) are coprime.
For each odd $p$, the totient $\phi(p^e)$ is even for all $e \geq 1$. So for $(\mathbb{Z}/n\mathbb{Z})^\times$ to be cyclic, $n$ can have at most one odd prime divisor. Also, $2 \mid \phi(2^e)$ for all $e \geq 2$. So the possible unit groups $(\mathbb{Z}/n\mathbb{Z})^\times$ that could be cyclic are

$$(\mathbb{Z}/2\mathbb{Z})^\times, \quad (\mathbb{Z}/4\mathbb{Z})^\times, \quad (\mathbb{Z}/p^e\mathbb{Z})^\times, \quad (\mathbb{Z}/2p^e\mathbb{Z})^\times.$$ 

We know that the first three groups in fact are cyclic. For $n = 2p^e$, the Sun Ze Theorem gives

$$(\mathbb{Z}/2p^e\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/p^e\mathbb{Z})^\times \cong (\mathbb{Z}/p^e\mathbb{Z})^\times,$$

showing that the fourth group is cyclic as well. If $g$ generates $(\mathbb{Z}/p^e\mathbb{Z})^\times$ then whichever of $g$ and $g+p^e$ is odd generates $(\mathbb{Z}/2p^e\mathbb{Z})^\times$. 