When is $\mathbb{Z}_n$ an integral domain? Is it commutative? Yes. Does it have identity? Yes. Zero divisors? No if n is prime. Yes otherwise.

Proposition

If p is prime, $\mathbb{Z}_p$ is a domain.

Proof

Suppose $ab = 0$ in $\mathbb{Z}_p$. Then $ab = 0 \mod p$. Then $p/(ab) \Rightarrow p/a$ or p/b which is a property of primes. So $a = 0$ or $b = 0$ in $\mathbb{Z}_p$. $\square$

Note. $\mathbb{Z}_1$ is not a domain because it doesn't have the identity.

20:

Theorem: Fermat's little theorem

If p is a prime and $a \in \mathbb{Z}, \gcd(a, p) = 1$, then $a^{p-1} = 1 \mod p$.

Equivalently, in $\mathbb{Z}_p$, if $a \neq 0$ then $a^{p-1} = 1$ in $\mathbb{Z}_p$.

Lemma: 1

If G is a finite group and $x \in G$ then $o(x)$ divides $|G|$. If $x^n = 1$, then $o(x)$ is a divisor of n.

Proof

If $k = o(x)$ then $n = qk + r$ for $0 \leq r < k$.

$$x^n = x^{qk+r} = x^r(x^k)^q = x^r e^q = x^r.$$

But since k is the smallest $m > 0$ with $x^m = e$. This means $r = 0 \Rightarrow k/n$. $\square$

Lemma: 2

If G is a finite group and $x \in G$, then $x^{|G|} = e$.

Because $o(x)/|G|$.

Question: how big is the group of units of $\mathbb{Z}_p$?

$(\mathbb{Z}_p)^*$ has order $p-1$.

Example. $(\mathbb{Z}_7)^* \simeq (\mathbb{Z}_6, +_6)$. In fact, this is generated by 3. Its inverse is also a generator, so 5. 3 or 5 is a primitive root modulo 7.

Proof

If $a \in (\mathbb{Z}_p)^*$ then $a^{|(\mathbb{Z}_p)^*|} = e$. Then $a^{p-1} = 1$ in $\mathbb{Z}_p$. $\square$

Example. Find the remainder of 8^{103} when divided by 13.

By F.l.T,

$$a^{p-1} = 1 \mod p \text{ if } \gcd(a,p) = 1.$$

Take $p = 13, a = 8, \gcd(8, 13) = 1$. So

$$\begin{aligned} 8^{12} &= 1 \mod 13 \\ 8^{24} = 8^{12^2} = 1^2 &= 1 \mod 13 \\ 8^{36} &= 1 \mod 13 \\ &\dots \\ 8^{96} &= 1 \mod 13 \end{aligned}$$

$$8^{103} = 8^{96} \times 8^7 \mod 13$$

If we track $8^k \mod 13$ for $k = 1, \dots, 7$, we get $8^7 = 5 \mod 13$. Therefore, $8^{103} = 5 \mod 13$.

Example. Show that $2^{11213} - 1$ is not divisible by 11. (This is actually the Mersenne prime, $2^p - 1$).

What is $2^{11213} \mod 11$? (We hope it's not 1).

By F.l.T, $2^{10} = 1 \mod 11$. Then we want a multiple of 10 just under the number. Then $2^{11210} = 1$. So $2^{11213} = 2^3 \times 2^{11210} = 8 \mod 11$.

Example. Show that $15/(n^{33} - n)$ for all $n \in \mathbb{Z}$.

Is 11215 a multiple of 15? The last digit is 5, but it's not a multiple of 3.