Example 124.

(a) Show that 7 is a primitive root modulo 26.

(b) Using the first part, make a complete list of all primitive roots modulo 26.

Solution.

(a) We need to show that 7 has order $\phi(26) = 12$.
The order of 7 (or any invertible residue) must divide $\phi(26) = 12$. Hence, the only possibilities for orders are $1, 2, 3, 4, 6, 12$. The fact that $7^4 \equiv (-3)^2 \equiv 9 \not\equiv 1 \pmod{26}$ and $7^6 \equiv (-3)^3 \equiv -1 \not\equiv 1 \pmod{26}$ is enough (why?!) to conclude that the order of 7 must be 12.

(b) Since 7 is a primitive root, all other invertible residues are of the form 7^a.
Recall that 7^a has order $\frac{12}{\gcd(12, a)}$. Thus, 7^a is a primitive root if and only if $\gcd(12, a) = 1$.
Therefore, a list of all primitive roots modulo 26 is: $7, 7^5, 7^7, 7^{11}$
[These are $\phi(\phi(26)) = \phi(12) = 4$ many primitive roots.]

The same logic applies whenever there is at least one primitive root:

Theorem 125. (number of primitive roots) Suppose there is a primitive root modulo n. Then there are $\phi(\phi(n))$ primitive roots modulo n.

Proof. Let x be a primitive root. It has order $\phi(n)$. All other invertible residues are of the form x^a.
Recall that x^a has order $\frac{\phi(n)}{\gcd(\phi(n), a)}$. This is $\phi(n)$ if and only if $\gcd(\phi(n), a) = 1$. There are $\phi(\phi(n))$ values a among $1, 2, \ldots, \phi(n)$, which are coprime to $\phi(n)$.
In conclusion, there are $\phi(\phi(n))$ primitive roots modulo n. □

Comment. Recall that, for instance, there is no primitive root modulo 8. That's why we needed the assumption that there should be a primitive root modulo n (which is the case if and only if n is of the form $1, 2, 4, p^k, 2p^k$ for some odd prime p).

Corollary 126. There are $\phi(\phi(p)) = \phi(p-1)$ primitive roots modulo a prime p.

Example 127. Let p be an odd prime. Show that at most half of the invertible residues modulo p are primitive roots.

Solution. In other words, we need to show that $\frac{\phi(p-1)}{p-1} \leqslant \frac{1}{2}$. Let $p_1, p_2, \ldots$ be the primes, in increasing order, dividing $p-1$. Since $p \neq 2$, $p-1$ is divisible by 2, so that $p_1 = 2$.

Then, $\phi(p-1) = (p-1)\underbrace{\left(1 - \frac{1}{p_1}\right)}_{=1/2}\underbrace{\left(1 - \frac{1}{p_2}\right)\cdots}_{\leqslant 1} \leqslant \frac{1}{2}(p-1)$.

Correspondingly, $\frac{\phi(p-1)}{p-1} \leqslant \frac{\frac{1}{2}(p-1)}{p-1} = \frac{1}{2}$, as claimed.

In fact. Note that $\left(1 - \frac{1}{p_2}\right) < 1$ if there is a second prime. Our proof therefore actually shows that $\frac{\phi(p-1)}{p-1} = \frac{1}{2}$ if and only if $p-1$ is of the form 2^n (i.e. the only prime dividing $p-1$ is 2). Equivalently, if p is of the form $2^n + 1$.

Comment. Primes of the form $2^n + 1$ are known as **Fermat primes**. It can be shown that such a prime is, in fact, necessarily of the form $F_k = 2^{2^k} + 1$. The first five numbers $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ are prime, and Fermat conjectured that F_k is prime for all $k \geqslant 0$. This was proven wrong by Euler who demonstrated that $F_5 = 2^{32} + 1 = 641 \cdot 6700417$ (this was way before the time, we could ask a computer to factor not-too-large numbers). To this day, it is not known whether any further Fermat primes exist.

Example 128. Recall that, for every prime p, primitive roots exist. The total number of primitive roots is $\phi(\phi(p)) = \phi(p-1)$. The following computations in Sage indicate that typically a "decent" proportion (25-50%) of all invertible residues are primitive roots. The exact proportion is, of course $\frac{\phi(p-1)}{p-1}$ but to say more about the magnitude, we need the factorization of $p-1$.

Advanced comment. However, the number of primitive roots can (though this is very rare) be an arbitrarily small proportion. In fact, a result of Kátai shows that, for any $x \in [0,1]$, there is a proportion $P(x)$ of primes with $\frac{\phi(p-1)}{p-1} \leqslant x$, and that $P(x)$ is a strictly increasing continuous function with $P(0)=0$ and $P(1/2)=1$.

```
Sage] prime_range(30)
```

$[2, 3, 5, 7, 11, 13, 17, 19, 23, 29]$

```
Sage] euler_phi(26)
```

12

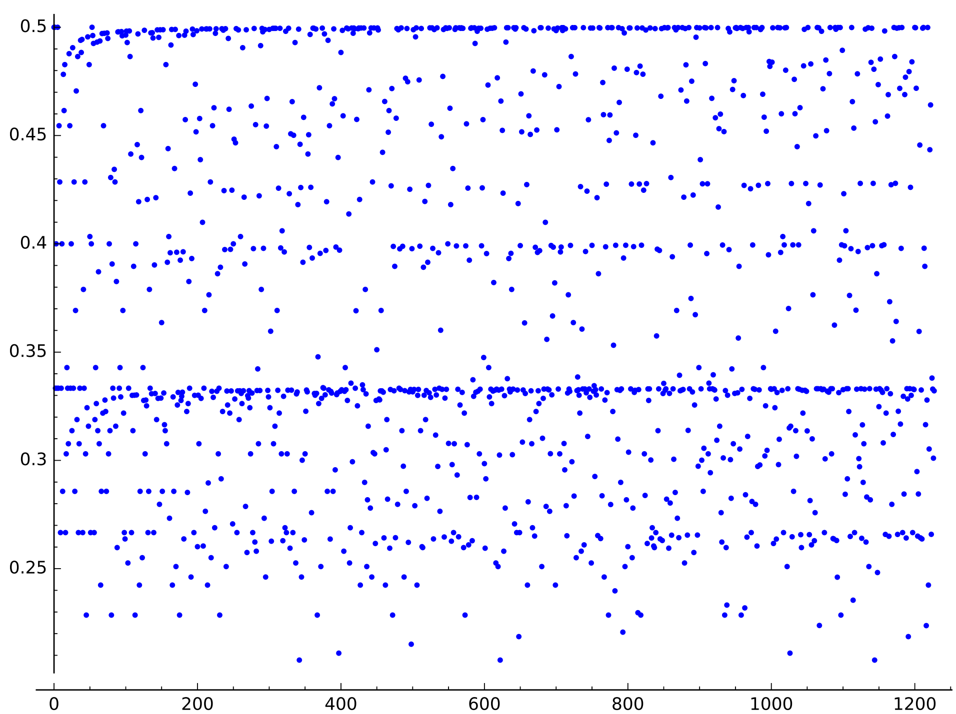
```
Sage] [p^2 for p in prime_range(30)]
```

$[4, 9, 25, 49, 121, 169, 289, 361, 529, 841]$

```
Sage] [euler_phi(p-1)/(p-1) for p in prime_range(30)]
```

$$\left[1, \frac{1}{2}, \frac{1}{2}, \frac{1}{3}, \frac{2}{5}, \frac{1}{3}, \frac{1}{2}, \frac{1}{3}, \frac{5}{11}, \frac{3}{7}\right]$$

```
Sage] list_plot([euler_phi(p-1)/(p-1) for p in prime_range(3,10000)])
```



Armin Straub
straub@southalabama.edu