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

Example 155. (extra) Let p be an odd prime. Show that the $\frac{\phi(p-1)}{p-1} \leqslant \frac{1}{2}$.

In other words, at most half of the invertible residues are primitive roots.

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

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 156. One can show that, for every prime p, primitive roots exist. By Example 154, it follows that 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 $P(1/2) = 1$.

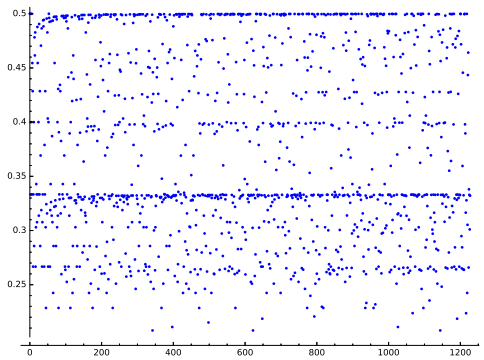
```
Sage] [p for p in prime_range(100)]
```

$$[2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97]$$

```
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)])
```



Safe primes

Recall that p is a safe prime if both p and $(p-1)/2$ are prime. The next example illustrates why it is common to use safe primes for ElGamal.

In general, it is difficult to ensure that g is a primitive root, or almost a primitive root, modulo p.

Example 157. Suppose that p is a safe prime. Show that all residues $g \not\equiv 0, \pm 1 \pmod{p}$ have order $(p-1)/2$ or $p-1$.

In the latter case, g is a primitive root. In fact, half of the residues $g \not\equiv 0, \pm 1$ are primitive roots.

Solution. Suppose $g \not\equiv 0, \pm 1 \pmod{p}$. Because p is a prime and $g \not\equiv 0$, g is invertible. Its multiplicative order N divides $\phi(p) = p-1$. But the prime factorization of $p-1$ is 2 times $(p-1)/2$. Hence, the only possible orders are $1, 2, (p-1)/2$ and $p-1$. The residues ± 1 are the only with order 1 and 2 (why?!). Thus, g must have order $(p-1)/2$ or $p-1$.

Finally, note that the number of primitive roots is $\phi(p-1) = \phi(2)\phi((p-1)/2) = (p-3)/2$, which is exactly half of the residues g.