ElGamal sobre $\mathbb{Z}_p$

Seja r uma raiz primitiva de p; ou seja,

$$\mathbb{Z}_p^* =< r >.$$

Ou seja, para todo $b \in \mathbb{Z}_p^*$, existe um único k com $1 \leq k \leq p-1$ para o qual $b = r^k \mod p$.

In [26]:
```
p = next_prime(10000)
Zp=IntegerModRing(p)
r = primitive_root(p)
r = Zp(r)
p, r
```

Out[26]: (10007, 5)

In [14]:
```
a = 17
b=Zp(r^a)
b
```

Out[14]: 9093

In [15]:
```
ChPub = (p, r, b)
ChPriv = a
```

In [16]:
```
mens = 1234
```

In [32]:
```
k = 1004
gama, delta = mens * b^k, r^k
```

In [33]:
```
gama, delta
```

Out[33]: (104, 3091)

In [34]:
```
delta^(-a)*gama
```

Out[34]: 1234

Para cifrar $mens$, Bob usa a chave pública de Alice; escolhe um k aleatoriamente, e calcula

$$(\gamma, \delta) = (mens \cdot b^k, r^k).$$

Alice, para decifrar o par (γ, δ), calcula

$$(\delta^{-1})^a \cdot \gamma.$$

In [ ]:
```

```