

$$E : y^2 = x^3 + Ax + B$$

$$-16(4A^3 + 27B^2) \neq 0$$

$$P \mapsto nP$$

$$1728 \frac{A^3}{4A^3 + 27B^2}$$

A pairing is a nondegenerate map  $e : G_1 \times G_2 \rightarrow G_3$ , where  $G_i$  are cyclic and  $|G_i| = p$  satisfying:

1.  $e(aP, bQ) = e(P, Q)^{ab}$
2.  $e(P, Q) \neq 1$  for some  $P, Q$
3.  $e$  is efficiently computable

The Weil Pairing:  $e : E(F_p)[r] \times E(F_p)[r] \rightarrow \mu_r$ , where  $E(F_p)[r]$  is the group of  $r$ -torsion points and  $\mu_r \subset \overline{F_p}$  are the  $r$ th roots of unity.

The Tate Pairing:  $\tau : E(F_p)[r] \times E(F_p)[r]/rE(F_p) \rightarrow \mu_r$

The Weil/Tate Pairing is efficiently computable when  $\mu_r \subset F_{p^k}$ , where  $k$  is small. This holds iff  $\gcd(r, p^k - 1) = r \iff p^k - 1 \equiv 0 \pmod r \iff p$  is a primitive  $k$ th root of unity mod  $r$ . A curve with efficiently computable pairings is *pairing-friendly*.

If  $r \approx p$ , then  $\Pr[\text{pairing-friendly curve}] = O(\frac{\log^3 M}{M})$