› Borevitch [4, p. 425]). Thus we may con-
›sition is true.

*Ɐ be an elliptic curve defined over* $\mathbf{Q}(\sqrt{-30})$.
*ient Galois module* $E_l$. *Then if t belongs to*
*me,* $|t|$ *belongs to* $\{2, 3, 5\}$.

hall carry out the descent arguments on
which were presupposed in this chapter.

IDEDNESS CONJECTURE

tudy the following conjecture of Ogg [23].

r $\mathbf{Q}$. IV.1.1. Let $E$ be an elliptic curve
group of $E_{\mathrm{tor}}(\mathbf{Q})$. Then $T$ is parametrizable.

ans that the modular curve classifying
a torsion structure $T$, that is, pairs $(E, T)$
ıus 0. There are 15 parametrizable torsion
er $\mathbf{Q}$, the 10 cyclic groups $Z/lZ$ ($l = 1, \ldots, 10$),
$\times Z/6Z$, $Z/2Z \times Z/2Z$, and $Z/2Z \times Z/4Z$.
which are parametrizable which cannot
luality, for example, $Z/3Z \times Z/3Z$ and

ıe following theorem.

*: an elliptic curve defined over* $\mathbf{Q}$. *Suppose*
*and l is a prime for which Fermat's last*
*:eds 3,* $l^2$ *does not divide the order of* $E_{\mathrm{tor}}(\mathbf{Q})$.
$\geqslant 23$ *such that l divides the order of* $E_{\mathrm{tor}}(\mathbf{Q})$.

ɜ first statement follows from the work of
5.5). The subgroup $Z/5Z \times Z/5Z$ is impos-
ıt no curve can have a 25-point over $\mathbf{Q}$ is
e proof will occupy a sizable portion of this

y be rephrased as saying that the only
volving exclusively primes less than 23 *are*
are 2, 3, 5, 7, 11, 13, 17, 19. By duality,
ıer be cyclic or $Z/2Z \times C$ where $C$ is cyclic.
$N$-cycle are parametrized by $H/\Gamma_0(N)$; for
24, 27, 32, 36, 49, the curve $X_0(N)$ has genus
iscussed by Ligozat [13]. From Ligozat's

Kubert, Daniel Sion
Universal bounds on the torsion of elliptic curves.
Proc. London Math. Soc. (3) 33 (1976), no. 2, 193–237.



paper, which, although not the earliest, is probably the most convenient reference, we see immediately that no elliptic curve over $\mathbf{Q}$ can have a torsion point defined over $\mathbf{Q}$ of any of these orders. Mazur and Tate [20], and independently Blass [3], recently proved that rational points of order 13 do not exist on elliptic curves defined over $\mathbf{Q}$. It is a classical (and easy) result of Lind [14] that points of order 16 are impossible.

Thus we need examine only torsion whose order involves the primes 2, 3, 5, 7. Cyclic torsion groups $Z/NZ$ exist and are parametrizable for $N = 1, \ldots, 10$ and $N = 12$, and the subgroup $Z/NZ \times Z/2Z$ exists and is parametrizable for $N = 2, 4, 6, 8$. The parametrizations are given in Table 3. Accordingly, it remains only to check that $Z/35Z$, $Z/10Z \times Z/2Z$,

TABLE 3. *Parametrization of torsion structures*

1. $0$: $y^2 = x^3 + ax^2 + bx + c$; $\Delta_1(a, b, c) \neq 0$,
   $\Delta_1(a, b, c) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$.
2. $Z/2Z$: $y^2 = x(x^2 + ax + b)$; $\Delta_1(a, b) \neq 0$, $\Delta_1(a, b) = a^2b^2 - 4b^3$.
3. $Z/2Z \times Z/2Z$: $y^2 = x(x+r)(x+s)$, $r \neq 0 \neq s \neq r$.
4. $Z/3Z$: $y^2 + a_1xy + a_3y = x^3$; $\Delta(a_1, a_3) = a_1{}^3a_3{}^3 - 27a_3{}^4 \neq 0$.

(The form $E(b, c)$ is used in all parametrizations below where in $E(b, c)$
$y^2 + (1-c)xy - by = x^3 - bx^2$, $(0, 0)$ is a torsion point of maximal order,
$\Delta(b, c) = \alpha^4b^3 - 8\alpha^2b^4 - \alpha^3b^3 + 36\alpha b^4 + 16b^5 - 27b^4$, and $\alpha = 1 - c$.)

5. $Z/4Z$: $E(b, c)$, $c = 0$, $\Delta(b, c) = b^4(1 + 16b) \neq 0$.
6. $Z/4Z \times Z/2Z$: $E(b, c)$, $b = v^2 - \frac{1}{16}$, $v \neq 0$, $\pm\frac{1}{4}$, $c = 0$.
7. $Z/8Z \times Z/2Z$: $E(b, c)$, $b = (2d-1)(d-1)$, $c = (2d-1)(d-1)/d$,
   $d = \alpha(8\alpha+2)/(8\alpha^2-1)$, $d(d-1)(2d-1)(8d^2-8d+1) \neq 0$.
8. $Z/8Z$: $E(b, c)$, $b = (2d-1)(d-1)$, $c = (2d-1)(d-1)/d$, $\Delta(b, c) \neq 0$.
9. $Z/6Z$: $E(b, c)$, $b = c + c^2$, $\Delta(b, c) = c^6(c+1)^3(9c+1) \neq 0$.
10. $Z/6Z \times Z/2Z$: $E(b, c)$, $b = c + c^2$, $c = (10-2\alpha)/(\alpha^2-9)$,
    $\Delta(b, c) = c^6(c+1)^3(9c+1) \neq 0$.
11. $Z/12Z$: $E(b, c)$, $b = cd$, $c = fd - f$, $d = m + \tau$, $f = m/(1-\tau)$,
    $m = (3\tau - 3\tau^2 - 1)/(\tau - 1)$, $\Delta(b, c) \neq 0$.
12. $Z/9Z$: $E(b, c)$, $b = cd$, $c = fd - f$, $d = f(f-1) + 1$, $\Delta(b, c) \neq 0$.
13. $Z/5Z$: $E(b, c)$, $b = c$, $\Delta(b, c) = b^5(b^2 - 11b - 1) \neq 0$.
14. $Z/10Z$: $E(b, c)$, $b = cd$, $c = fd - f$, $d = f^2/(f-(f-1)^2)$, $f \neq (f-1)^2$, $\Delta(b, c) \neq 0$.
15. $Z/7Z$: $E(b, c)$, $b = d^3 - d^2$, $c = d^2 - d$, $\Delta(b, c) = d^7(d-1)^7(d^3 - 8d^2 + 5d + 1) \neq 0$.

$Z/25Z$, $Z/18Z$, and $Z/12Z \times Z/2Z$ are impossible. The cases $Z/10Z \times Z/2Z$ and $Z/12Z \times Z/2Z$ are easy, since such curves would be 2-isogenous to one with a rational 20-cycle or a rational 24-cycle and so correspond to a point of $X_0(20)$ or $X_0(24)$. The cases $Z/35Z$, $Z/25Z$, and $Z/18Z$ are dealt with explicitly below.