and use H as the basis of an inductive argument. This function has the following properties:

- For any $K > 0$ the set $\{P \in \mathcal{G} : H(P) < K\}$ is finite.
- For each $Q \in \mathcal{G}$ there exists a constant c depending only on Q such that $H(P+Q) \leq c(H(P))^2$.
- There exists a constant d such that $H(P) \leq d(H(2P))^{1/4}$.
- The quotient group $\mathcal{G}/2\mathcal{G}$ is finite.

In fact, if $P = (x, y)$ and $x = m/n$ in lowest terms, we take $H(P) = \max(|m|, |n|)$. □

Recall from Proposition 1.18 that a finitely generated abelian group is of the form

$$F \oplus \mathbf{Z}^k$$

where F is a finite abelian group, hence a direct sum of finite cyclic groups. The group F, which is unique, consists of the elements of finite order, and is called the *torsion subgroup*. The groups $\mathcal{G}$ determined by elliptic curves are very special, as is shown by the following theorem of Mazur:

Theorem 13.20. *Let $\mathcal{G}$ be the group of rational points on an elliptic curve. Then the torsion subgroup of $\mathcal{G}$ is isomorphic either to Z_l where $1 \leq l \leq 10$, or $Z_2 \oplus \mathbf{Z}_{2l}$ where $1 \leq l \leq 4$.*

Proof: The proof is very technical: see Mazur [48, 49]. □

13.7 Applications to Diophantine Equations

We now describe an application of the above ideas to an equation very similar to Fermat's. This application is due to Elkies [23].

We know that it is impossible for two cubes to sum to a cube, but might it be possible for three cubes to sum to a cube? It is; in fact $3^3+4^3+5^3 = 6^3$. Euler conjectured that in general n nth powers can sum to an nth power, but not $n-1$. It has been proved that Euler's conjecture is false. In 1966 L. J. Lander and T. R. Parkin [42] found the first counterexample to Euler's conjecture: four fifth powers whose sum is a fifth power. In fact

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

As a check:

$$
\begin{array}{rcl}
27^5 & = & 14348907 \\
84^5 & = & 4182119424 \\
110^5 & = & 16105100000 \\
133^5 & = & 41615795893 \\
\hline
144^5 & = & 61917364224.
\end{array}
\tag{13.10}
$$

They found this example by exhaustive computer search.

In 1988 Noam Elkies found another counterexample by applying the theory of elliptic curves: three fourth powers whose sum is a fourth power.

$$
\begin{array}{rcl}
2682440^4 & = & 51774995082902409832960000 \\
15365639^4 & = & 55744561387133523724209779041 \\
18796760^4 & = & 124833740909952854954805760000 \\
\hline
20615673^4 & = & 180630077292169281088848499041
\end{array}
\tag{13.11}
$$

Instead of looking for integer solutions to the equation $x^4 + y^4 + z^4 = w^4$, Elkies divided out by w^4 and looked at the surface $r^4 + s^4 + t^4 = 1$ in coordinates (r, s, t). An integer solution to $x^4 + y^4 + z^4 = w^4$ leads to a rational solution $r = x/w, s = y/w, z = t/w$ of $r^4 + s^4 + t^4 = 1$. Conversely, given a rational solution of $r^4 + s^4 + t^4 = 1$, we can assume that r, s, t all have the same denominator w by putting them over a common denominator, and that leads directly to a solution to $x^4 + y^4 + z^4 = w^4$. Demjanenko [19] had found a rather complicated condition for a rational point (r, s, t) to lie on the closely related surface $r^4 + s^4 + t^2 = 1$. Namely, such a rational point exists if and only if there exist x, y, u such that

$$
\begin{aligned}
r &= x + y \\
s &= x - y \\
(u^2 + 2)y^2 &= -(3u^2 - 8u + 6)x^2 - 2(u^2 - 2)x - 2u \\
(u^2 + 2)t &= 4(u^2 - 2)x^2 + 8ux + (2 - u^2)
\end{aligned}
$$

To solve Elkies's problem it is enough to show that t can be made a square. A series of simplifications shows that this can be done provided the equation

$$Y^2 = -31790X^4 + 36941X^3 - 56158X^2 + 28849X + 22030$$

has a rational solution. This equation defines an elliptic curve. (Despite the presence of a fourth power on the right hand side, it can be transformed into a cubic. A similar transformation can be found in Section 14.2. See also McKean and Moll [52] page 254.) Conditions are known under which no solution can exist, but these conditions did not hold in this case, which