Доказательства Ферма до нас не дошли, однако в тех случаях, когда он утверждал, что доказал ту или иную теорему, впоследствии эту теорему удавалось доказать. Единственным исключением является следующее утверждение: «Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duas ejusdem nominis fas est dividere; cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet» («Невозможно разложить куб на два куба, или биквадрат на два биквадрата, или вообще степень, большую двух, на две степени с тем же самым показателем; я нашел этому поистине чудесное доказательство, однако поля слишком узки, чтобы оно здесь вместилось»).

Этот текст, сопровождаемый указанием: «Наблюдение господина Пьера де Ферма», содержится в издании трудов Диофанта, которое было выпущено Ферма-сыном в 1670 году, через 5 лет после смерти отца. Это подлинное замечание, внесенное Ферма в его собственный экземпляр трудов Диофанта, в настоящее время утраченный. Каждому, кто держал в руках «Арифметику» Диофанта издания 1621 года, бросаются в глаза необычайно широкие поля – возможно, именно по этой причине Пьер Ферма записывал на них свои замечания.

Таким образом, в переводе на современный математический язык, Ферма утверждал, что уравнение

$$a^n + b^n = c^n, \quad n > 2,$$

не имеет целочисленных решений с $abc \neq 0$. Это утверждение называется *последней* (или *великой*) *теоремой Ферма*. В настоящее время все специалисты твердо уверены в том, что Ферма не обладал доказательством этой теоремы и, сверх того, что элементарными методами ее нельзя доказать.

Более трехсот лет теорема Ферма привлекала внимание многих поколений математиков и служила беспрецедентным стимулом для развития математики. Для показателей $n = 3$ и $n = 4$ неразрешимость уравнения $a^n + b^n = c^n$ была доказана Эйлером (опубликовано в 1770 году). Честь доказательства великой теоремы Ферма для $n = 5$ разделили в 1825 году два выдающихся математика: немец Дирихле, который только что достиг двадцати лет и как раз начинал свою блестящую научную карьеру, и француз Лежандр – всемирно известный специалист в теории чисел и анализе. В 1832 году, через семь лет после того, как был доказан случай $n = 5$, Дирихле опубликовал доказательство случая $n = 14$. Разумеется, это слабее случая $n = 7$, поскольку любая 14-я степень является 7-й степенью, но не наоборот, и это доказательство было своего рода признанием неудачи со случаем $n = 7$. Прошло еще семь лет, прежде чем в 1839 году французский математик Ламе опубликовал доказательство для $n = 7$. Все эти доказательства технически очень сложны, однако их методы, по существу, элементарны. В 1847 году немецкий математик Куммер создал теорию «идеального разложения», позволившую одним приемом доказать теорему Ферма для всех простых показателей, меньших 100, кроме $n = 37$, 59 и 67. Начиная с этого времени основные усилия математиков были направлены на нахождение все более мощных достаточных условий, при которых выполняется теорема Ферма. Были разработаны разнообразные средства, приведшие к созданию обширного раздела математики – теории алгебраических чисел. С помощью сложнейшей теоретико-числовой техники теорема Ферма была проверена для всех $n \leq 4\,000\,000$, но до конца 1994 года в общем случае оставалась недоказанной. Получить ее полное доказательство удалось лишь с помощью теории эллиптических кривых. Поэтому мы начнем с краткого экскурса в эту теорию [2].

Эллиптические кривые

Рассмотрим плоскую кривую, заданную уравнением третьей степени

$$f(x,y) = \alpha_{30}x^3 + \alpha_{21}x^2y + \ldots$$

$$\ldots + \alpha_1 x + \alpha_2 y + \alpha_0 = 0. \quad (1)$$

Все такие кривые естественным образом разбиваются на два класса. К первому классу относятся те кривые, у которых имеются точки заострения (типа точки (0; 0) у кривой $y^2 = x^3$, рис.1), самопересечения (как точка (0; 0) у кривой $y^2 = x^3 + x^2$, рис.2), а также кривые, для которых многочлен $f(x,y)$ представляется в виде

$$f(x,y) = f_1(x,y) \cdot f_2(x,y),$$

где $f_1(x,y)$, $f_2(x,y)$ – многочлены меньших степеней (пример приведен на рисунке 3). Кривые этого класса называются *вырожденными* кривыми третьей степени. Второй класс кривых образуют невырожденные кривые; мы будем называть их *эллиптическими*. Если коэффициенты многочлена (1) – рациональные числа, то эллиптическая кривая может быть преобразована к так называемой канонической форме

$$y^2 = x^3 + ax + b. \quad (2)$$

Типичный вид такой кривой изображен на рисунках 4 и 5.

С каждой эллиптической кривой можно связать важную числовую характеристику – ее *дискриминант*.

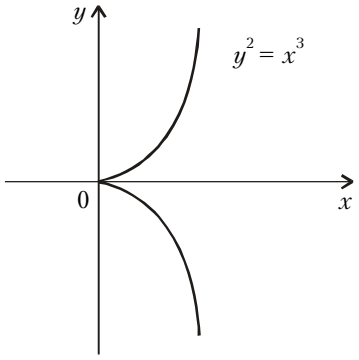

Рис.1

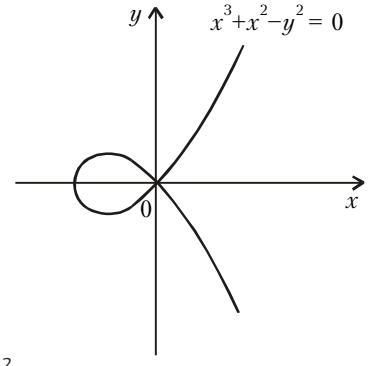

Рис.2

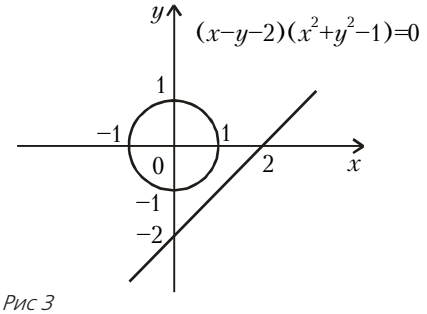

Рис.3