Elementary Number Theory

Section 3.3 Sums of two squares

Definition 3.3.1 We list four functions:

(a) $R(n)$: the number of ordered pairs (x, y) of integers such that $x^2 + y^2 = n$;

(b) $r(n)$: the number of ordered pairs (x, y) of integers such that $(x, y) = 1$ and $x^2 + y^2 = n$;

(c) $P(n)$: the number of proper representations of n by the form $x^2 + y^2$ for which $x > 0$ and $y \geq 0$.

(d) $N(n)$: the number of solutions of the congruence $s^2 \equiv -1 \pmod{n}$.

Example 3.3.2 $H(-4) = 1$. Thus $x^2 + y^2$ is the only positive definite binary quadratic form with discriminant -4.

Theorem 3.3.3 A positive integer n is properly representable as a sum of two squares if and only if the prime factors of n are all of the form $4k + 1$, except for the prime 2, which may occur to at most the first power.

Remark 3.3.4 Reprove Theorem 2.1.31.

Write the canonical factorization of n in the form

$$n = 2^\alpha \prod_{p \equiv 1 \pmod{4}} p^\beta \prod_{q \equiv 3 \pmod{4}} q^\gamma.$$

Then n can be expressed as a sum of two squares of integers if and only if all the exponents γ are even.

Theorem 3.3.5 Suppose that $n > 0$. Then

(a) $r(n) = 4P(n)$;

(b) $P(n) = N(n)$;

(c) $R(n) = \sum r(\frac{n}{d^2})$ where the sum is extended over those positive d for which $d^2 | n$.

Theorem 3.3.6 Let $n = 2^\alpha \prod p p^\beta \prod q^\gamma$ where p runs over prime divisors of n of the form $4k + 1$, and q runs over prime divisors of n of the form $4k + 3$.

(a) $r(n) = \begin{cases} 2^{t+2} & \text{if } \alpha = 0 \text{ or } 1 \text{ and all } \gamma \text{ are } 0, \\ 0 & \text{otherwise }, \end{cases}$ where t is the number of primes p of the form $4k + 1$ that divides n.

(b) $R(n) = \begin{cases} 4 \prod_p (\beta + 1), & \text{if all the } \gamma \text{ are even }, \\ 0 & \text{otherwise }. \end{cases}$

Corollary 3.3.7 The number of representations of a positive integer n as a sum of two squares is 4 times the excess in the number of divisors of n of the form

$4k+1$ over those of the form $4k+3$. That is, $R(n) = 4\sum\left(\frac{-1}{d}\right)$, where d runs over the positive odd divisors over n.

Example 3.3.8 Find integers x and y such that $x^2 + y^2 = p$ where $p = 398417$ is a prime.

Theorem 3.3.9 Let f be a positive definite binary quadratic form of discriminant $d < 0$.

(a) $R_f(n)$= the number of representations of n by f.

(b) $r_f(n)$= the number of proper representations of n by f.

(c) $H_f(n) = |\{h : 0 \leq h < 2n, h^2 = d + 4nk$ and the form $nx^2 + hxy + ky^2$ is equivalent to $f\}|$.

(d) $N_d(n) = |\{h : 0 \leq h < 2n, h^2 \equiv d(\mod 4n)\}|$.

Theorem 3.3.10 Let f be a positive definite binary quadratic form with discriminant $d < 0$. Then for any $n \in \mathbb{N}$, $r_f(n) = w(f)H_f(n)$, and $R_f(n) = \sum_{m^2|n} r_f(\frac{n}{m^2})$.

Remark 3.3 11 Let $\mathcal{F}$ be the set of all reduced positive definite binary quadratic form with discriminant $d < 0$. Then $\sum_{f\in\mathcal{F}} H_f(n) = N_d(n)$.

For many discriminants d it happens that $W(f) = \omega$ is a constant for all $f \in \mathcal{F}$. Thus $\sum_{f\in\mathcal{F}} r_f(n) = \omega N_d(n)$. It is not easy to describe $r_f(n)$.