Chapter 8. Some Diophantine Equations

Differences of Two Squares

8.1 Theorem: *(Differences of Two Squares) Let $n \in \mathbb{Z}^+$.*
(1) There exists a solution $(x,y) \in \mathbb{Z}^2$ to the Diophantine equation $x^2 - y^2 = n$ if and only if n is odd or n is a multiple of 4.
(2) In the case that n is odd, the number of solutions is equal to $2\,\tau(n)$ and the solutions are given by $(x,y) = \big(\pm\frac{s+r}{2}, \pm\frac{s-r}{2}\big)$ where $n = rs$ with $0 < r \leq s$.
(3) In the case that n is a multiple of 4, the number of solutions is $2\,\tau\big(\frac{n}{4}\big)$, and the solutions are given by $(x,y) = \big(\pm(\ell+k), \pm(\ell-k)\big)$ where $n = 4k\ell$ with $0 < k \leq \ell$.

Proof: For $x,y \in \mathbb{Z}_4$ we have $x^2 \in \{0,1\}$ and $y^2 \in \{0,1\}$, and so $x^2 - y^2 \in \{0,1,3\}$. Thus for $n \in \mathbb{Z}$, if $n = x^2 - y^2$ for some $x,y \in \mathbb{Z}$ then $n \in \{0,1,3\}$ mod 4, that is either n is odd or n is a multiple of 4. When n is odd, say $n = 2k+1$, we can take $x = k+1$ and $y = k$ to get $x^2 - y^2 = (k+1)^2 - k^2 = 2k+1 = n$. When n is a multiple of 4, say $n = 4k$, we can take $x = k+1$ and $y = k-1$ to get $x^2 - y^2 = (k+1)^2 - (k-1)^2 = 4k = n$. Thus for $n \in \mathbb{Z}$, the Diophantine equation $x^2 - y^2 = n$ has a solution if and only if either n is odd or n is a multiple of 4.

When $n = 0$ we have $x^2 - y^2 = n \iff x^2 - y^2 = 0 \iff x^2 = y^2 \iff y = \pm x$ and so there are infinitely many solutions, namely $(x,y) = (r,r)$, $r \in \mathbb{Z}$.

Since $x^2 - y^2 = -n \iff y^2 - x^2 = n$, it follows that the number of solutions to the equation $x^2 - y^2 = -n$ is equal to the number of solutions to the equations $x^2 - y^2 = n$, so it suffices to consider the case that $n > 0$. Also note that if $x^2 - y^2 = n$ then we also have $(\pm x)^2 - (\pm y)^2 = n$ so it suffices to count the number of solutions $(x,y) \in \mathbb{Z}^2$ with $0 \leq y < x$. We must multiply the number of solutions with $0 < y < x$ by 4 and, in the case that n is a square, we also have the 2 solutions $(x,y) = \big(\pm\sqrt{n}, 0\big)$.

Suppose that $n \in \mathbb{Z}^+$ and that either n is odd or n is a multiple of 4. Note that $x^2 - y^2 = n \iff (x-y)(x+y) = n$. Given $x,y \in \mathbb{Z}$ with $0 \leq y < x$ such that $x^2 - y^2 = n$, we can let $r = x - y$ and $s = x + y$ and then we have $0 < r \leq s$ and $rs = n$ and $s - r = 2y$ so that $r = s$ mod 2. On the other hand, given $r,s \in \mathbb{Z}$ with $0 < r \leq s$ and $rs = n$ and $r = s$ mod 2, we can let $x = \frac{s+r}{2}$ and $y = \frac{s-r}{2}$ and then we have $0 < y \leq x$ and $x^2 - y^2 = (x-y)(x+y) = rs = n$. Thus there is a bijective correspondence between pairs $(x,y) \in \mathbb{Z}^2$ with $0 < y \leq x$ such that $x^2 - y^2 = n$ and pairs $(r,s) \in \mathbb{Z}^2$ with $0 < r \leq s$ and $rs = n$ and $r = s$ mod 2. In the case that n is a square, the pair (x,y) with $y = 0$ corresponds to the pair (r,s) with $r = s$.

When n is odd and $rs = n$, both r and s are odd so that we have $r = s$ mod 2. When n is not a square, $\tau(n)$ is even and the number of pairs $(r,s) \in \mathbb{Z}^2$ with $0 < r \leq s$ and $rs = n$ is equal to $\frac{\tau(n)}{2}$. In this case, the total number of solutions $(x,y) \in \mathbb{Z}^2$ is equal to $4 \cdot \frac{\tau(n)}{2} = 2\tau(n)$. When n is a square, $\tau(n)$ is odd and we obtain 1 pair (r,s) with $r = s$ and $\frac{\tau(n)-1}{2}$ pairs (r,s) with $r < s$. In this case, the total number of solutions $(x,y) \in \mathbb{Z}^2$ is $2 + 4 \cdot \frac{\tau(n)-1}{2} = 2\tau(n)$. In either case, the total number of solutions is $2\tau(n)$.

When n is a multiple of 4, say $n = 4m$, to get $rs = n$ with $r = s$ mod 2, the factors r and s must both be even, say $r = 2k$ and $s = 2\ell$. The number of required pairs (r,s) is equal to the number of pairs $(k,\ell) \in \mathbb{Z}^2$ with $0 < k \leq \ell$ and $k\ell = m$. As above, whether or not m is a square, the total number of solutions $(x,y) \in \mathbb{Z}^2$ is equal to $2\tau(m)$.

Sums of Two Squares

8.2 Note: Our main goal in this section is to determine for which integers $n \in \mathbb{Z}$ there exists a solution $(x,y) \in \mathbb{Z}^2$ to the Diophantine equation $x^2 + y^2 = n$ and, for such n, to determine the number of solutions. In our analysis of the simpler equation $x^2 - y^2 = n$ we made use of the factorization $x^2 - y^2 = (x-y)(x+y)$. In our analysis of the equation $x^2 + y^2 = n$ we shall find it useful to work in the ring of Gaussian integers $\mathbb{Z}[i] = \{a + ib \,|\, a, b \in \mathbb{Z}\}$ and to make use of the factorization $x^2 + y^2 = (x - iy)(x + iy)$.

Let us recall some facts about the ring $\mathbb{Z}[i]$ from Chapter 6. Recall that $\mathbb{Z}[i]$ is a Euclidean domain, hence a unique factorization domain, with Euclidean norm equal to the field norm N in $\mathbb{Q}[i]$. For $x, y \in \mathbb{Q}$ and $u = x + iy \in \mathbb{Q}[i]$, we have

$$N(u) = u\overline{u} = \|u\|^2 = x^2 + y^2.$$

The norm is multiplicative, meaning that $N(uv) = N(u)N(v)$ for all $u, v \in \mathbb{Q}[i]$. The units in $\mathbb{Z}[i]$ are the elements $u \in \mathbb{Z}[i]$ with $N(u) = 1$, namely the 4 elements ± 1 and $\pm i$, and the non-zero non-units are the elements $u \in \mathbb{Z}[i]$ with $N(u) > 1$. The associates of the element $u \in \mathbb{Z}[i]$ are the elements $\pm u$ and $\pm iu$. Because $\mathbb{Z}[i]$ is a unique factorization domain, the prime elements in $\mathbb{Z}[i]$ are the same as the irreducible elements in $\in \mathbb{Z}[i]$. Finally, note that for $u \in \mathbb{Z}[i]$, if $N(u)$ is a prime number in $\mathbb{Z}^+$ then u must be irreducible in $\mathbb{Z}[i]$ because if we had $u = vw \in \mathbb{Z}[i]$ with v and w being nonzero nonunits, then we would have $N(u) = N(v)N(w) \in \mathbb{Z}^+$ with $N(u) > 1$ and $N(w) > 1$.

8.3 Theorem: *(Irreducible Elements in the Ring of Gaussian Integers) Every irreducible element in the ring $\mathbb{Z}[i]$ is an associate of exactly one of the following elements.*
(1) $1 + i$,
(2) p, *where p is a prime number in $\mathbb{Z}^+$ with* $p = 3 \bmod 4$,
(3) $x \pm iy$, *where $x, y \in \mathbb{Z}$ with $0 < y < x$ and $x^2 + y^2 = p$ for some prime number $p \in \mathbb{Z}^+$ with* $p = 1 \bmod 4$.

Proof: Our first claim is that for a prime number $p \in \mathbb{Z}^+$, p is reducible in $\mathbb{Z}[i]$ if and only if $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$. Let p be a prime number in $\mathbb{Z}^+$. Suppose first that p is reducible in $\mathbb{Z}[i]$. Choose nonzero nonunits $u, v \in \mathbb{Z}[i]$ such that $p = uv$. Since u and v are nonzero nonunits we have $N(u) > 1$ and $N(v) > 1$, and since $N(u)N(v) = N(uv) = N(p) = p^2$ we must have $N(u) = p$ and $N(v) = p$. Write $u = x + iy$ with $x, y \in \mathbb{Z}$. Then we have $p = N(u) = x^2 + y^2$. Suppose, conversely, that $p = x^2 + y^2$ where $x, y \in \mathbb{Z}$. Let $u = x + iy$ and $v = x - iy$. Then $N(u) = N(v) = p$ so that u and v are nonzero nonuits, and we have $uv = x^2 + y^2 = p$ so that p is reducible.

Note that 2 is reducible in $\mathbb{Z}[i]$ with $2 = (1+i)(1-i)$. Our second claim is that when p is an odd prime number in $\mathbb{Z}^+$, p is reducible in $\mathbb{Z}[i]$ if and only if $p = 1 \bmod 4$. Let p be an odd prime number in $\mathbb{Z}^+$ and note that (since p is odd) either $p = 1 \bmod 4$ or $p = 3 \bmod 4$. Since $0^2 = 2^2 = 0 \bmod 4$ and $1^2 = 3^2 = 1 \bmod 4$, for all $x \in \mathbb{Z}$ we have $x^2 \in \{0, 1\} \bmod 4$. It follows that for all $x, y \in \mathbb{Z}$ we have $x^2 + y^2 \in \{0+0, 0+1, 1+1\} = \{0, 1, 2\} \bmod 4$. Thus when $p = 3 \bmod 4$ there do not exist $x, y \in \mathbb{Z}$ such that $x^2 + y^2 = p$ so, by our first claim, we know that p is irreducible. On the other hand, when $p = 1 \bmod 4$ we know from Chapter 4 that $-1 \in Q_p$ so we can choose $x \in \mathbb{Z}^+$ such that $x^2 = -1 \bmod p$, say $x^2 = -1 + kp$ with $k \in \mathbb{Z}^+$. Then in $\mathbb{Z}[i]$ we have $kp = x^2 + 1 = (x+i)(x-i)$. If p was irreducible in $\mathbb{Z}[i]$, then by unique factorization, either $p \big| (x+i)$ or $p \big| (x-i)$, but this is not the case because (working in $\mathbb{Q}[i]$) the elements $\frac{x \pm i}{p}$ do not lie in $\mathbb{Z}[i]$, so p is reducible.

Our third claim is that each element $q\in\mathbb{Z}[i]$ which is of one of the types 1, 2 and 3 (in the statement of the theorem) is irreducible in $\mathbb{Z}[i]$. When q is of type 1, that is when $q=1+i$, we have $N(q)=2$ (which is prime in $\mathbb{Z}^+$) and so q is irreducible in $\mathbb{Z}[i]$ (by the last remark in Note 8.2). When q is of type 2, that is when $q=p$ for some prime number $p\in\mathbb{Z}^+$ with $p=3 \bmod 4$, then we know that q is irreducible from our second claim. When q is of type 3, that is when $q=x\pm iy$ where $x,y\in\mathbb{Z}$ with $0<y\leq x$ and $x^2+y^2=p$ for some prime number $p\in\mathbb{Z}^+$ with $p=1 \bmod 4$, then we have $N(q)=x^2+y^2=p$, which is prime in $\mathbb{Z}^+$, so q must be irreducible in $\mathbb{Z}[i]$ (by the final remark in Note 8.2 again).

Our fourth claim is that every irreducible element $q\in\mathbb{Z}[i]$ is an associate of a unique element of one of the three types. Let q be an irreducible element in $\mathbb{Z}[i]$. Since the units in $\mathbb{Z}[i]$ are the elements ±1 and $\pm i$, it follows that the 4 associates of q (which are also irreducible) are obtained by rotating q bout the origin by a multiple of $\frac{\pi}{2}$, and so q has a unique associate $x+iy$ which lies in the quarter-plane given by $-x<y\leq x$. When $y=x$ we have $x+iy=x(1+i)$ with $x\in\mathbb{Z}^+$, and for this to be irreducible we must have $x=1$ so that $x+iy=1+i$, which is of type 1. When $y=0$ we have $x+iy=x$ with $x\in\mathbb{Z}^+$ and, for this to be irreducible in $\mathbb{Z}[i]$, we must have x irreducible in $\mathbb{Z}^+$ so that $x+iy=x=p$ for some prime number $p\in\mathbb{Z}^+$ and, again for this to be irreducible in $\mathbb{Z}[i]$, we must have $p=3 \bmod 4$, which is of type 2. Otherwise (that is when $y\neq x$ and $y\neq 0$) we have $-x<y<0$ or $0<y<x$, so we can say that q has a unique associate of the form $x\pm iy$ with $0<y<x$. In this case, factor $N(q)=x^2+y^2=q\overline{q}$ in $\mathbb{Z}^+$ to get $q\overline{q}=p_1p_2\cdots p_\ell$ with each p_k a prime number in $\mathbb{Z}^+$. Since q is irreducible in $\mathbb{Z}[i]$, by unique factorization in $\mathbb{Z}[i]$, we must have $q\big|p_k$ in $\mathbb{Z}[i]$ for some index k. Say $q\big|p$ in $\mathbb{Z}[i]$ where $p=p_k$ is a prime number in $\mathbb{Z}^+$. Since $q\big|p$ in $\mathbb{Z}[i]$ we have $N(q)\big|N(p)$, that is $N(q)\big|p^2$, in $\mathbb{Z}^+$. Since $N(q)>1$ we must have $N(q)=p$ or $N(q)=p^2$. In the case that $N(q)=p^2$, since $q\big|p$ in $\mathbb{Z}[i]$ and $N(q)=N(p)=p^2$ it follows that $\frac{p}{q}\in\mathbb{Z}[i]$ with $N\big(\frac{p}{q}\big)=1$, and hence $\frac{p}{q}$ is a unit in $\mathbb{Z}[i]$, so q is an associate of p, which is of type 2. In that case that $N(q)=p$ we have $p=N(q)+N(x+iy)=x^2+y^2$ so that q is an associate of $x+iy$, which is of type 3.

8.4 Corollary: *(Sums of Two Squares) Let $n\in\mathbb{Z}^+$ factor as $n=2^m\cdot\prod\limits_\alpha {p_\alpha}^{k_\alpha}\cdot\prod\limits_\beta {q_\beta}^{\ell_\beta}$ where $m\in\mathbb{N}$, $k_\alpha,\ell_\beta\in\mathbb{Z}^+$, the p_α are distinct primes with $p_\alpha=1 \bmod 4$, and the q_β are distinct primes with $q_\beta=3 \bmod 4$. Then there exists a solution $(x,y)\in\mathbb{Z}^2$ to the Sum of Two Squares Equation $x^2+y^2=n$ if and only if each exponent ℓ_β is even, and in this case, the number of solutions $(x,y)\in\mathbb{Z}^2$ is equal to $4\cdot\prod\limits_\alpha(k_\alpha+1)$.*

Proof: Note that for $x,y\in\mathbb{Z}$, we have $x^2+y^2=n$ in $\mathbb{Z}$ if and only if $(x+iy)(x-iy)=n$ in $\mathbb{Z}[i]$. Thus the number of pairs $(x,y)\in\mathbb{Z}^2$ such that $x^2+y^2=n$ is equal to the number of elements $u=x+iy\in\mathbb{Z}[i]$ such that $n=u\overline{u}$. By the above theorem, n factors in $\mathbb{Z}[i]$ into irreducibles as

$$n=(1+i)^m(1-i)^m\cdot\prod_\alpha {v_\alpha}^{k_\alpha}\,{\overline{v}_\alpha}^{k_\alpha}\cdot\prod_\beta {q_\beta}^{\ell_\beta}=(-i)^m(1+i)^{2m}\cdot\prod_\alpha {v_\alpha}^{k_\alpha}\,{\overline{v}_\alpha}^{k_\alpha}\cdot\prod_\beta {q_\beta}^{\ell_\beta}.$$

To get $n=u\overline{u}$, u must be a factor of n in $\mathbb{Z}[i]$. The factors of n in $\mathbb{Z}[i]$ are

$$u=e\cdot(1+i)^a\cdot\prod_\alpha {v_\alpha}^{b_\alpha}{\overline{v}_\alpha}^{c_\alpha}\cdot\prod_\beta {q_\beta}^{d_\beta}$$

where $e\in\{\pm1,\pm i\}$, $0\leq a\leq m$, $0\leq b_\alpha\leq k_\alpha$, $0\leq c_\alpha\leq k_\alpha$ and $0\leq d_\beta\leq\ell_\beta$, and for the above factor u we have $u\overline{u}=1\cdot2^a\cdot\prod\limits_\alpha {p_\alpha}^{b_\alpha+c_\alpha}\cdot\sum\limits_\beta {q_\beta}^{2d_\beta}$, so in order to get $u\overline{u}=n$ we need $e\in\{\pm1,\pm i\}$ (there are 4 choices for e), we need $a=m$ (so there are no choices for a), we need $b_\alpha+c_\alpha=k_\alpha$ (so there are $k_\alpha+1$ choices for the pair (b_α,c_α)) and we need $2d_\beta=\ell_\beta$ (so each ℓ_β must be even and there are no choices for d_α).

Pell's Equation

8.5 Note: In this section we discuss **Pell's equation**, which is the Diophantine equation $x^2 - dy^2 = 1$ where $d \in \mathbb{Z}^+$ is a non-square. In Chapters 6 and 7 we have already done all of the work necessary to solve this equation. Let us recall some of the relevant facts.

It is useful to work in the real quadratic ring $\mathbb{Z}[\sqrt{d}\,]$. For $u = x + y\sqrt{d} \in \mathbb{Q}[\sqrt{d}\,]$ with $x, y \in \mathbb{Q}$, we write $\overline{u} = x - y\sqrt{d}$ and we use the field norm in $\mathbb{Q}[\sqrt{d}\,]$ given by

$$N(u) = u\overline{u} = x^2 - dy^2.$$

The norm is multiplicative, meaning that $N(uv) = N(u)N(v)$. The units in $\mathbb{Z}[\sqrt{d}\,]$ are the elements $u \in \mathbb{Z}[\sqrt{d}\,]$ with $N(u) = \pm 1$, that is the elements $u = x + y\sqrt{d}$ with $x, y \in \mathbb{Z}$ such that $x^2 - dy^2 = \pm 1$ (almost, but not quite, the same as the solutions to Pell's equation). When $x, y \in \mathbb{Z}$ and $u = x + y\sqrt{d}$ is a unit in $\mathbb{Z}[\sqrt{d}\,]$, we have $u > 1$ if and only if $x, y \in \mathbb{Z}^+$. There is a unique smallest unit $u \in \mathbb{Z}[\sqrt{d}\,]$ with $u > 1$, and (all of) the units in $\mathbb{Z}[\sqrt{d}\,]$ are the elements of the form $\pm u^k$ with $k \in \mathbb{Z}$. When u is this unique smallest unit with $u > 1$, either we have $N(u) = 1$ or we have $N(u) = -1$. In the case that $N(u) = 1$ we have $N(\pm u^k) = 1$ for all $k \in \mathbb{Z}$ so (all of) the solutions to Pell's equation are given by $(x, y) = (\pm r_k, \pm s_k)$ where $u^k = r_k + s_k\sqrt{d}$. In the case that $N(u) = -1$ we have $N(\pm u^k) = (-1)^k$ so the smallest unit $v \in \mathbb{Z}[\sqrt{d}\,]$ with $v > 1$ and with $N(v) = 1$ is $v = u^2$ and (all of) the solutions to Pell's equation are given by $(x, y) = (\pm r_{2k}, \pm s_{2k})$ where $v^k = u^{2k} = r_k + s_k\sqrt{d}$.

When d is fairly small, the smallest unit $u \in \mathbb{Z}[\sqrt{d}\,]$ with $u > 1$ can be found using trial and error (simply try values of $y \in \mathbb{Z}^+$ until $dy^2 \pm 1$ is a square, say $dy^2 \pm 1 = x^2$, and then the smallest such unit is $u = x + y\sqrt{d}\,$). When d is large, trial and error can become quite tedious, but we can calculate u using continued fractions. We calculate the continued fraction for $\sqrt{d}$ and the convergents $\frac{p_k}{q_k}$. If we let $u_k = p_k + q_k\sqrt{d}$ then the smallest unit $u \in \mathbb{Z}[\sqrt{d}\,]$ with $u > 1$ is $u = u_{\ell-1}$ where ℓ is the minimum period of the continued fraction.

8.6 Example: Solve Pell's equation $x^2 - 53y^2 = 1$.

Solution: We calculate the continued fraction for $\sqrt{53}$ and the first few convergents $c_k = \frac{p_k}{q_k}$ along with the norms $N_k = N(p_k + q_k\sqrt{53}) = p_k^2 - 53\,q_k^2$.

k	x_k	a_k	p_k	q_k	N_k
0	$\sqrt{53}$	7	7	1	-4
1	$\frac{1}{\sqrt{53}-7} = \frac{\sqrt{53}+7}{4}$	3	22	3	7
2	$\frac{4}{\sqrt{53}-5} = \frac{\sqrt{53}+5}{7}$	1	29	4	-7
3	$\frac{7}{\sqrt{53}-2} = \frac{\sqrt{53}+2}{7}$	1	51	7	4
4	$\frac{7}{\sqrt{53}-5} = \frac{\sqrt{53}+5}{4}$	3	182	25	-1
5	$\frac{4}{\sqrt{53}-7} = \frac{\sqrt{53}+7}{1}$	14			

We have $\sqrt{53} = [7, \overline{3, 1, 1, 3, 14}]$ with period $\ell = 5$. Writing $u_k = p_k + q_k\sqrt{53} \in \mathbb{Z}[\sqrt{53}\,]$, the smallest unit in $\mathbb{Z}[\sqrt{53}\,]$ with $u > 1$ is $u = u_{\ell-1} = u_4 = 182 + 25\sqrt{53}$, and we have $N(u) = -1$. The smallest unit v in $\mathbb{Z}[\sqrt{53}\,]$ with $v > 1$ and $N(v) = 1$ is

$$v = u^2 = (182 + 25\sqrt{53})^2 = 66\,249 + 9\,100\sqrt{53}.$$

If we write $v^k = (66\,249 + 9\,100\sqrt{53})^k = r_k + s_k\sqrt{53}$ for $0 \le k \in \mathbb{Z}$, then the solutions to Pell's equation $x^2 - 53y^2 = 1$ are given by $(x, y) = (\pm r_k, \pm s_k)$ where $0 \le k \in \mathbb{Z}$.

Pythagorean Triples

8.7 Note: In this section we study the Diophantine equation $x^2+y^2=z^2$. The solutions given by $x=0$ and $z\pm y$ and by $y=0$ and $z=\pm x$ are called the **trivial solutions**. If (x,y,z) is a solution, then so are $(\pm x,\pm y,\pm z)$. A solution (x,y,z) with $x,y,z\in\mathbb{Z}^+$ is called a **Pythagorean triple**. Note that if (x,y,z) is a Pythagorean triple and $r\in\mathbb{Z}^+$ then $r(x,y,z)=(rx,ry,rz)$ is also a Pythagorean triple and, likewise, if (x,y,z) is a Pythagorean triple and $d=\gcd(x,y,z)$, then $\frac{1}{d}(x,y,z)$ is also a Pythagorean triple. A **primitive Pythagorean triple** is a Pythagorean triple (x,y,z) with $\gcd(x,y,z)=1$. Note that when (x,y,z) is a primitive Pythagorean triple, one of the numbers x and y is even and the other is odd (if both were odd we would have $z^2=x^2+y^2=1+1=2\in\mathbb{Z}_4$).

8.8 Theorem: *(Pythagorean Triples) The Pythagorean triples (x,y,z), with x even, are of the form*

$$(x,y,z)=r\big(2st,s^2-t^2,s^2+t^2\big)$$

for some uniquely determined $r,s,t\in\mathbb{Z}^+$ with $s>t$, $\gcd(s,t)=1$ where s and t are not both odd.

Proof: Note that when $(x,y,z)\in\mathbb{Z}^3$ with $x^2+y^2=z^2$ and $z\neq 0$, we have $\left(\frac{x}{z}\right)^2+\left(\frac{y}{z}\right)^2=1$ so that the point $\left(\frac{x}{z},\frac{y}{z}\right)$ is a point on the unit circle with rational coordinates. Let S be the unit circle $S=\big\{(x,y)\in\mathbb{R}^2\,|\,x^2+y^2=1\big\}$ and let $T=S\setminus\{(0,1)\}$. The **stereographic projection** from T to $\mathbb{R}$ is the function $f:T\to\mathbb{R}$ defined as follows: given $(a,b)\in T$, let $f(a,b)=u$ where u is the real number such that $(u,0)$ lies on the line through $(0,1)$ and (a,b). The inverse map $g:\mathbb{R}\to T$ is given as follows: Given $u\in\mathbb{R}$, we let $g(u)=(a,b)$ where (a,b) is the (unique) point on T which lies on the line through $(0,1)$ and $(u,0)$. Let us find a formula for f and a formula for its inverse g.

Given $(a,b)\in T$, the line from $(0,1)$ to (a,b) is given parametrically by $(x,y)=(0,1)+t((a,b)-(0,1))=(ta,1+t(b-1))$. We have $(ta,1+t(b-1))=(u,0)$ when $1+t(b-1)=0$, that is $t=\frac{1}{1-b}$, and $u=ta=\frac{a}{1-b}$. Thus the map f is given by

$$u=f(a,b)=\tfrac{a}{1-b}\,.$$

Given $u\in\mathbb{R}$, the line through $(0,1)$ and $(u,0)$ is given parametrically by $(x,y)=(0,1)+t((u,0)-(0,1))=(tu,1-t)$. The point $(a,b)=(tu,1-t)$ lies on S when $1=a^2+b^2=(tu)^2+(1-t)^2=t^2u^2+1-2t+t^2$, that is when $(u^2+1)t^2=2t$, or equivalently when $t=0$ or $t=\frac{2}{u^2+1}$. When $t=0$ the resulting point is $(a,b)=(tu,1-t)=(0,1)$ and when $t=\frac{2}{u^2+1}$ the resulting point is $(a,b)=(tu,1-t)=\left(\frac{2u}{u^2+1},\frac{u^2-1}{u^2+1}\right)$. Thus the inverse map g is given by

$$(a,b)=g(u)=\left(\tfrac{2u}{u^2+1},\tfrac{u^2-1}{u^2+1}\right).$$

Verify that $f\big(g(u)\big)=u$ for all $u\in\mathbb{R}$, and that $g\big(f(a,b)\big)=(a,b)$ for all $(a,b)\in T$.

Notice that if $(a,b)\in T$ with $a,b\in\mathbb{Q}$ then $u=f(a,b)\in\mathbb{Q}$ and that, conversely, if $u\in\mathbb{Q}$ then $(a,b)=g(u)\in\mathbb{Q}^2$. It follows that we have a bijective correspondence between $T\cap\mathbb{Q}^2$ and $\mathbb{Q}$ given by $f:T\cap\mathbb{Q}^2\to\mathbb{Q}$ and $g:\mathbb{Q}\to T\cap\mathbb{Q}^2$. Thus every element in $T\cap\mathbb{Q}^2$ is of the form

$$(a,b)=g\left(\tfrac{s}{t}\right)=\left(\tfrac{2(s/t)}{(s/t)^2+1},\tfrac{(s/t)^2-1}{(s/t)^2+1}\right)=\left(\tfrac{2st}{s^2+t^2},\tfrac{s^2-t^2}{s^2+t^2}\right)$$

for some $s,t\in\mathbb{Z}$ with $t\neq 0$ and $\gcd(s,t)=1$. Putting $s\neq 0$ and $t=0$ in the term on the right gives $(a,b)=(0,1)$, so we can say that every point $(a,b)\in S\cap\mathbb{Q}^2$ $\big($including the point $(a,b)=(0,1)\big)$ is of the form $a=\frac{x}{z}$ and $b=\frac{y}{z}$ with

$$(x,y,z)=\big(2st,s^2-t^2,s^2+t^2\big)$$

for some $s,t\in\mathbb{Z}$ with $\gcd(s,t)=1$.

Notice that when s and t are both odd, the values of $x = 2st$, $y = s^2 - t^2$ and $z = s^2 + t^2$ are all even so that the fractions $a = \frac{x}{z}$ and $b = \frac{y}{z}$ are not in reduced form. In this case we can divide x, y and z by 2, or equivalently, we can interchange x and y and replace s and t by $s' = \frac{s+t}{2}$ and $t' = \frac{s-t}{2}$ (which are both integers) because

$$\begin{aligned} x' &= 2s't' = 2\left(\tfrac{s+t}{2}\right)\left(\tfrac{s-t}{2}\right) = \tfrac{s^2-t^2}{2} = \tfrac{y}{2}\,, \\ y' &= (s')^2 - (t')^2 = \left(\tfrac{s+t}{2}\right)^2 - \left(\tfrac{s-t}{2}\right)^2 = st = \tfrac{x}{2}\ \text{, and} \\ z' &= (s')^2 + (s')^2 = \left(\tfrac{s+t}{2}\right)^2 + \left(\tfrac{s-t}{2}\right)^2 = \tfrac{s^2+y^2}{2} = \tfrac{z}{2}. \end{aligned}$$

It follows that every Pythagorean triple (x, y, z) with x even is of the form

$$(x, y, z) = r\big(2st, s^2 - t^2, s^2 + t^2\big)$$

for some $s, t \in \mathbb{Z}^+$ with $s > t$ and $\gcd(s, t) = 1$ where s and t are not both odd.

It remains to verify that the positive integers s and t, as above, are uniquely determined. The key fact to verify is that in the case $r = 1$, so that $(x, y, z) = \big(2st, s^2-t^2, s^2+t^2\big)$ with s and t as above, we must have $\gcd(x, y, z) = 1$. Indeed, note that since $\gcd(s, t) = 1$ so that s and t are not both even, and since s and t are not both odd, it follows that $y = s^2 - t^2$ and $z = s^2 + t^2$ are both odd so that 2 cannot be a factor of either y or z. And when p is an odd prime, p cannot be a common factor of both y and z because if we had $p\big|y = (s^2 - t^2)$ and $p\big|z = (s^2 + t^2)$ then we would have $p\big|((s^2 + t^2) + (s^2 - t^2)) = 4s^2$ so that $p\big|s$ and we would have $p\big|((s^2 + t^2) - (s^2 - t^2)) = 4t^2$ so that $p\big|t$, but this is not possible since $\gcd(s, t) = 1$. Thus when $s, t \in \mathbb{Z}^+$ with $s > t$ and $\gcd(s, t) = 1$ and with s and t not both odd, the Pythagorean triple $\big(2st, s^2 - t^2, s^2 + t^2\big)$ is primitive. Thus for

$$(x, y, z) = r\big(2st, s^2 - t^2, s^2 + t^2\big)$$

with $r \in \mathbb{Z}^+$, the value of r is uniquely determined by $r = \gcd(x, y, z)$ and then s and t are uniquely determined by the two equations $s^2 + t^2 = \frac{z}{r}$ and $s^2 - t^2 = \frac{y}{r}$ which can be added to give $2s^2 = \frac{z+y}{2r}$ and subtracted to give $2t^2 = \frac{z-y}{2r}$.

8.9 Example: List all primitive pythagorean triples (x, y, z) with x even and $z \le 100$.

Solution: We list all pairs $(s, t) \in \mathbb{Z}^2$ with $1 \le t < s$ and $s^2 + t^2 \le 100$, then we cross off the pairs with $\gcd(s, t) > 1$ and the pairs with s and t both odd. We find 15 such pairs, and for each pair we calculate $(x, y, z) = \big(2st, s^2 - t^2, s^2 + t^2\big)$ and display the result in the following table (to save space we have listed the triples (x, y, z) vertically).

s	2	4	6	8	3	5	7	9	4	8	5	7	9	6	8
t	1	1	1	1	2	2	2	2	3	3	4	4	4	5	5
x	4	8	12	16	12	20	28	36	24	48	40	56	72	60	80
y	3	15	35	63	5	21	45	77	7	55	9	33	65	11	39
z	5	17	37	65	13	29	53	85	25	73	41	65	97	61	89

8.10 Example: We notice that $z = 65$ occurs twice in the above table in the triples $(x, y, z) = (16, 63, 65), (56, 33, 65)$. Note that $65 = 5 \cdot 13$, so from the Sums of Two Squares Theorem, we know that there are $4 \cdot 3 \cdot 3 = 36$ pairs $(x, y) \in \mathbb{Z}^2$ such that $x^2 + y^2 = 65^2$. Note that 4 of these pairs are given by $(x, y) = (\pm 65, 0), (0, \pm 65)$ and the other 32 pairs can be grouped into sets of 4 pairs of the form $(\pm x, \pm y)$ with $x, y \in \mathbb{Z}^+$. Thus there should be 8 pairs (x, y) with $x, y \in \mathbb{Z}^+$ such that $x^2 + y^2 = 65^2$. There are 4 such pairs (x, y) with x even and 4 such pairs with y even. Two of the 4 pairs (x, y) with x even occur in the two primitive Pythagorean triples $(x, y, z) = (16, 63, 65), (56, 33, 65)$. The other two pairs occur in the non-primitive Pythagorean triples $(x, y, z) = 13(4, 3, 5)$ and $5(12, 5, 13)$.

Fermat's Last Theorem

I may include some notes on Fermat's Last Theorem later.