ON THE SUM OF TWO COPRIME SQUARES

GERGELY HARCOS

We shall use the action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half-plane to count the number of ways a given positive integer can be written as a sum of two coprime squares. The ideas here can also be used to efficiently find such a representation when it exists and the prime factorization of the given positive integer is known.

Our starting point is Euler's identity [1]

$$(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2.$$

Amusingly, Euler used the exact same letters, which will be convenient for us when forming a matrix from them. For $a,b,c,d\in\mathbb{Z}$, the above identity shows that c^2+d^2 divides the right-hand side. In particular, if $ad-bc=1$, then the pair

$$(m,n):=(ac+bd,c^2+d^2)\in\mathbb{Z}\times\mathbb{Z}_{\geqslant 1} \tag{1}$$

satisfies $n\mid m^2+1$. In other words, the residue class m mod n is a square-root of -1 mod n.

In fact every pair $(m,n)\in\mathbb{Z}\times\mathbb{Z}_{\geqslant 1}$ satisfying $n\mid m^2+1$ arises this way. To see this, we recall the action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half-plane:

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}z:=\frac{az+b}{cz+d},\qquad \begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z}),\quad \Im(z)>0.$$

If we fix $z=i$, then this action is given by

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}i=\frac{ai+b}{ci+d}=\frac{(ac+bd)+i}{c^2+d^2},\qquad \begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z}). \tag{2}$$

For later reference we remark that the map (2) is 4-to-1:

$$\begin{pmatrix}a'&b'\\c'&d'\end{pmatrix}i=\begin{pmatrix}a&b\\c&d\end{pmatrix}i\quad\Longleftrightarrow\quad\begin{pmatrix}a'&b'\\c'&d'\end{pmatrix}\in\left\{\pm\begin{pmatrix}a&b\\c&d\end{pmatrix},\pm\begin{pmatrix}b&-a\\d&-c\end{pmatrix}\right\}. \tag{3}$$

So our claim amounts to showing that for every pair $(m,n)\in\mathbb{Z}\times\mathbb{Z}_{\geqslant 1}$ satisfying $n\mid m^2+1$, the point $(m+i)/n$ is equivalent to i under the action of $\mathrm{SL}_2(\mathbb{Z})$.

To verify the last claim, we apply a familiar variant of the Euclidean algorithm to move the point $(m+i)/n$ into the standard fundamental domain

$$\{z\in\mathbb{C}:\ |\Re z|\leqslant 1/2 \text{ and } |z|\geqslant 1\}.$$

Initially, we shift $(m+i)/n$ by a suitable integer to achieve $|m|\leqslant n/2$. If $n=1$, then $m=0$, so the point $(m+i)/n$ equals i. Otherwise, we apply the map $z\mapsto -1/z$ on $(m+i)/n$. The resulting point

$$\frac{-n}{m+i}=\frac{(-m+i)n}{m^2+1}=\frac{-m+i}{(m^2+1)/n}$$

is of the same shape as before, but with a smaller positive integer denominator:

$$(m^2+1)/n\leqslant n/4+1/n\leqslant n/2.$$

Iterating these steps, we end up with the point i in $O(\log(|m|+n))$ steps, and we are done.

The image of a right coset

$$\left\{\begin{pmatrix}1&k\\&1\end{pmatrix}:k\in\mathbb{Z}\right\}\begin{pmatrix}a&b\\c&d\end{pmatrix}=\left\{\begin{pmatrix}*&*\\c&d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})\right\}$$

under the map (2) yields a single $n = c^2 + d^2$ and a whole residue class m mod n satisfying $m^2 + 1 \equiv 0 \pmod{n}$, cf. (1). By (3), there are precisely 4 right cosets yielding a given positive integer n and a given square-root of -1 modulo n, and these correspond to 4 primitive lattice points (c,d), $(d,-c)$, $(-c,-d)$, $(-d,c)$ forming a square centered at the origin. Hence we proved the following

Theorem (Gauss). *Let n be a positive integer. Then the number of primitive integral solutions of $n = c^2 + d^2$ equals 4 times the number of square-roots of -1 modulo n.*

Corollary (Gauss). *Let n be a positive integer. If n is of the form $p_1^{r_1} \cdots p_k^{r_k}$ or $2p_1^{r_1} \cdots p_k^{r_k}$ with distinct primes $p_j \equiv 1 \pmod{4}$, then the number of primitive integral solutions of $n = c^2 + d^2$ equals 2^{k+2}. Otherwise, there are no primitive integral solutions of $n = c^2 + d^2$.*

References

[1] L. Euler, *De numeris, qui sunt aggregata duorum quadratorum*, Novi Commentarii Academiae Scientiarum Imperialis Petropolitanae **4** (1758), 3–40, available at https://www.biodiversitylibrary.org/page/40612490; English translation by P. R. Bialek available at https://scholarlycommons.pacific.edu/euler-works/228

Alfréd Rényi Institute of Mathematics, POB 127, Budapest H-1364, Hungary
Email address: gharcos@renyi.hu