Seminar of Elementary Number Theory

Jean-Luc Portner and Matthias Schmickler

October 8, 2021

1 Introduction

The goal of chapter 2 is presenting a way to prove that any integer can be represented as a sum of four squares. In order to do this, we will prove several results such as a criterion for a number to be representable as a sum of two squares and introduce the concept of Legendre symbols and quadratic residues. Chapter 3 will then prove a formula for calculating in how many ways a natural number can be represented as a sum of eight squares. Therefore, it will take a look at the Eisenstein series, theta series and eventually lead to Jacobi's formula.

2 Quadratic residues and the representation of a number as a sum of four squares

2.1 Definition of quadratic residues and the Legendre symbol

Definition 2.1. Let p be an odd prime (prime and $\neq 2$) and a an integer such that $ggT(a,p) = 1$. If there exists an integer x such that $x^2 \equiv a\ (modp)$ then a is called a quadratic residue modulo p. If there exists no such x, then a is called a quadratic non-residue modulo p. We write aRp if a is a quadratic residue modulo p and aNp if its a quadratic non-residue modulo p.

We want to know how many integers of $1, 2, 3, ..., p-1$ are quadratic residues modulo p. Consider

$$1^2, 2^2, 3^2, ..., \left(\frac{p-1}{2}\right)^2$$

which are the candidates for x^2.

Step 1: First of all we realize, that these numbers are all mutually incongruent mod p. Reason: if $r^2 \neq s^2$ and $r \neq s$ then $r^2 \equiv s^2$ mod p would imply that $r \equiv s$ mod p or $r \equiv -s$ mod p. Those possibilities are both excluded since $1 \leq r, s \leq \frac{p-1}{2}$.

Step 2: Further, $r^2 \equiv (p-r)^2$ mod p.

Step 3: Therefore it follows from these Steps that a in $x^2 \equiv a$ mod p assumes $\frac{p-1}{2}$ different values, when x runs through the set $1, 2, 3, ..., p-1$. Hence there are exactly $\frac{p-1}{2}$ quadratic residues modulo p and $\frac{p-1}{2}$ quadratic non-residues modulo p.

Definition 2.2. Let p be an odd prime and m an integer such that $ggT(m,p) = 1$. We define the Legendre symbol $\left(\frac{m}{p}\right)$ by the relations

$$\left(\frac{m}{p}\right) = \begin{cases} +1 & \text{if } mRp \\ -1 & \text{if } mNp. \end{cases}$$

We can extend the definition by defining $\left(\frac{m}{p}\right) = 0$ if $p|m$.

It follows that $\sum_{m=0}^{p-1} \left(\frac{m}{p}\right) = 0$ since we have as many quadratic residues as we have quadratic non-residues. Furthermore if $m_1 = m_2$ mod p we have $\left(\frac{m_1}{p}\right) = \left(\frac{m_2}{p}\right)$.

2.2 Wilson Theorem and Euler Criterion

Theorem 2.3 (Wilson Theorem)**.** *If p is a prime, then $(p-1)! \equiv -1$ mod p.*

Proof of Wilson Theorem. If $p = 2$ the conclusion is obvious. Let $p \geq 3$ we know that F_p is a field, therefore know that for every

$$x \in \{1, 2, 3, ..., p-1\} \; \exists! x' \in \{1, 2, 3, ..., p-1\} \text{ s.t. } x \cdot x' = 1 \bmod p. \quad (1)$$

Furthermore we know that $x = x'$ if and only if $x = 1$ or $x = p - 1$. Since

$$x^2 \equiv 1 \bmod p \iff (x-1)(x+1) \equiv 0 \bmod p$$

we know that

$$x = 1 \text{ or}$$

$$x \equiv -1 \bmod p \iff x = p - 1.$$

From (1) we know that $2 \cdot 3...(p-2) \equiv 1 \bmod p$ which we can multiply with $1 \cdot (p-1) \equiv -1 \bmod p$ which leads to $1 \cdot 2 \cdot 3...(p-1) \equiv -1 \bmod p$ which concludes the proof. □

Note that if p would be a composite e.g. $p = q \cdot r$ then, since $1 < q < p$ and therefore q and r occur in the product $1 \cdot 2 \cdot ...(p-1)$ we know that neither

$$(p-1)! + 1 \equiv 0 \bmod q \text{ nor}$$

$$(p-1)! + 1 \equiv 0 \bmod p$$

are possible. Thus Wilson's theorem states a property characteristic of the primes.

Theorem 2.4 (Euler's criterion)**.** *Suppose p is an odd prime and a is any integer. Then $a^{(p-1)/2} \equiv 1$ mod p if and only if a is a quadratic residue modulo p.*

For the proof we need two results:

Theorem 2.5 (Fermat's Theorem)**.** *If p is a prime and $ggT(a, p) = 1$ then $a^{p-1} \equiv 1$ mod p.*

Proof of Fermat's Theorem. The proof follows directly from the proof of the Lagrange Theorem for groups. The Lagrange theorem states, that every element of a group raised to the power of the order $(p-1)$ of the group is 1. □

Theorem 2.6 (Lagrange's Theorem)**.** *The congruence $a_0 x^n + a_1 x^{n-1} + ... + a_n \equiv 0$ mod p with $ggT(a_0, p) = 1$ has at most n solutions.*

Proof of Lagrange's Theorem. We use induction. The theorem is true for $n = 1$, since $gcd(a_0, p) = 1$. Now suppose the theorem is true with $n - 1$ in place of n. It is trivially true for the degree n, if the congruence

$$a_0 x^n + a_1 x^{n-1} + ... + a_n \equiv 0 \bmod p \text{ with } ggT(a_0, p) = 1$$

has no solution.

If it does have a solution, say x_1, then

$$a_0 x_1^n + a_1 x_1^{n-1} + ... + a_n \equiv 0 \bmod p$$

If we subtract this from the equation before then we get

$$a_0(x^n - x_1^n) + a_1(x^{n-1} - x_1^{n-1}) + ... + a_{n-1}(x - x_1) \equiv 0 \bmod p.$$

This equation is obviously satisfied by all the solutions of

$$a_0x^n + a_1x^{n-1} + ... + a_n \equiv 0 \bmod p \text{ with } ggT(a_0, p) = 1$$

. But it can be written as

$$(x - x_1)(a_0x^{n-1} + b_1x^{n-2} + ... + b_{n-1}) \equiv 0 \bmod p$$

where $b_1, b_2, ..., b_{n-1} are integers which dependon x_1$, and on the integers $a_0, ..., a_{n-1}$. Therefore every solution of

$$a_0x^n + a_1x^{n-1} + ... + a_n \equiv 0 \bmod p \text{ with } ggT(a_0, p) = 1$$

must satisfy either the congruence

$$(x - x_1) \equiv 0 \bmod p$$

which yields the original solution $x = x_1$ or

$$a_0x^{n-1} + b_1x^{n-2} + ... + b_{n-1} \equiv 0 \bmod p, gcd(a_0, p) = 1$$

which is of degree $n - 1$, and has by the induction hypothesis at most $n - 1$ solutions. In either case we get have at most n solutions, as claimed. □

Proof of Euler's criterion. We know that the equation $x^2 \equiv a \bmod p$ is solved by the quadratic residues. If we raise this equation to the power $(p - 1)/2$ (which is an integer since p is odd). Therefore we get $x^{(p-1)} \equiv a^{(p-1)/2} \bmod p$. By Fermat's theorem we know $x^{p-1} \equiv 1 \bmod p$ and hence $a^{(p-1)/2} \equiv 1 \bmod p$. On the other hand, the congruence $x^{(p-1)/2} \equiv 1 \bmod p$ has at most $(p-1)/2$ solutions by Lagrange's theorem. Since we know that there are exactly $(p-1)/2$ quadratic residues which satisfy the equation, which leads to the conclusion that there are no other solutions then the quadratic residues. □

Theorem 2.7. *If p is an odd prime, then $m^{(p-1)/2} \equiv \left(\frac{m}{p}\right)$ mod p.*

Proof. If p is an odd prime and $ggT(x,p) = 1$ then by Fermat's theorem

$$x^{p-1} - 1 = (x^{(p-1)/2} - 1)(x^{(p-1)/2} + 1) \equiv 0 \bmod p.$$

Hence either

$$x^{(p-1)/2} \equiv 1 \bmod p \ (2) \ or$$
$$x^{(p-1)/2} \equiv -1 \bmod p \ (3) \ .$$

But by Euler's criterion we know that (2) can not be true for a quadratic non-residue so it must satisfy (3). Now just use the definition of the Legendre symbol and we conclude. □

Corollary 2.8. *We have* $\left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = \left(\frac{mn}{p}\right)$

Note that this means that the product of two quadratic residues or non-residues modulo p, is again a quadratic residue; but the product of a quadratic residue with a quadratic non-residue, modulo p, is again a quadratic non-residue.

2.3 Sum of two squares

Now we are going to see why everything we have seen so far is actually important. The Euler Theorem and the theorem stating a condition for an integer to be representable as a sum of two squares are two very important applications of the theory of quadratic residues.

Theorem 2.9 (Euler)**.** *Every prime of the form $p = 4k + 1$ is representable as a sum of two squares.*

For the proof we need another result:

Theorem 2.10. *If n and A are positive integers, such that $n|(A^2 + 1)$ then there exist integers s and t, such that $n = s^2 + t^2$*

Proof. The case $n = 1$ is trivial. We assume therefore that $n \geq 2$, and define $N = [\sqrt{n}]$. Then $n > N$ for $n \geq 2$. Since $n|(A^2 + 1)$, it follows that $gcd(n, A) = 1$. Hence A/n is a reduced fraction with denominator $n > N$, and then there exists a reduced fraction r/s, such that

$$|\frac{A}{n} - \frac{r}{s}| \leq \frac{1}{(N+1)s}, 0 < s \leq N.$$

That is

$$|As - rn| \leq \frac{n}{N+1} = \frac{n}{[\sqrt{n}]+1} < \sqrt{n}.$$

Let $As - rn = t$. Then t is an integer, and

$$s^2 + t^2 = s^2 + (As - rn)^2 = s^2(A^2 + 1) - 2Asrn + r^2n^2.$$

Since n divides the right-hand side of the equation, we must have $n|(s^2 + t^2)$. But $0 < s \leq N \leq \sqrt{n}$, and $|t| < \sqrt{n}$, which together imply that $0 < s^2 + t^2 < 2n$. Since $s^2 + t^2$ is a multiple of n, we must have $s^2 + t^2 = n$, so that n is representable as a sum of two squares. □

Proof of Euler's theorem. Let p be an odd prime and set $m = p - 1$. From a previous Theorem we know that

$$m^{(p-1)/2} \equiv \left(\frac{m}{p}\right) \bmod p.$$

Since $p-1 \equiv -1 \bmod p$ we get

$$\left(\frac{m}{p}\right) \equiv (-1)^{(p-1)/2} \bmod p$$

But

$$\left(\frac{-1}{p}\right) = \pm 1, (-1)^{(p-1)/2} = \pm 1 \text{ and } p \geq 3$$

Hence

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$$

and therefore it follows that -1 is a quadratic residue mod p of all primes $p \equiv 1 \bmod 4$ and a quadratic non-residue mod p of all prime $p \equiv 3 \bmod 4$.

Since now $p = 4k+1$ we know that -1 is a quadratic residue of p. It follows $x^2 \equiv -1 \bmod p$ has a solution. Therefore there exists an integer A such that $p|(A^2+1)$ and by the Theorem mentioned above it follows that p is a sum of two squares. □

Theorem 2.11. *If p is a prime such that $p \equiv 1$ mod 4 then there exists an integer x such that $x^2+1 = mp$ for $0 < m < p$.*

Proof. Since -1 is a quadratic residue of p there exists an integer x of the set $1, 2, 3, ..., (p-1)/2$ which satisfies the congruence $x^2 \equiv -1 \bmod p$. That is $x^2+1 = mp$ for some integer m. But $x < p/2$ therefore $x^2+1 < (p/2)^2+1 < p^2$. Hence $x^2+1 = mp$ with $0 < m < p$. □

Theorem 2.12. *If p is an odd prime, there exist integers x and y such that $1+x^2+y^2 = mp$ where $0 < m < p$.*

Proof. The integers in $A = \{x^2 | 0 \leq x \leq (p-1)/2\}$ are pairwise incongruent mod p as are the integers in $B = \{-1-y^2 | 0 \leq y \leq (p-1)/2\}$. Together these sets contain p+1 integers but for only p residue classes. Therefore some $x^2 \in A$ must be congruent to some $-1-y^2 \in B$. Thus $x^2 \equiv -1-y^2 \bmod p$ or equivalently $1+x^2+y^2 = mp$.

$$0 \leq x, y \leq (p-1)/2 \Rightarrow 1+x^2+y^2 < 1+2(p/2)^2 < p^2$$

hence $1+x^2+y^2 = mp$ for $0 < m < p$ and we conclude. □

Till now we still haven't proved a sufficient condition for a positive integer to be representable as a sum of two squares. The next theorem is a result that resolves this problem.

Theorem 2.13. *A positive integer n is a sum of two squares if and only if all its prime factors of the form $4k+3$ have even exponents in the standard form of n.*

To prove this we need the following two lemmas.

Definition 2.14. We call a representation $n = x^2+y^2$ primitive if $ggT(x,y) = 1$ and imprimitive otherwise.

Lemma 2.15. *If n is divisible by a prime p where $p \equiv 3$ mod 4 then n has no primitive representation.*

Proof. If n has a primitive representation:

$$n = x^2+y^2 \text{ with } ggT(x,y) = 1 \Rightarrow p|(x^2+y^2) \text{ but } p \nmid x \text{ and } p \nmid y.$$

And since $ggT(p,x)=1$ the equation $mx-tp=c$ is solvable in integers m and t for all integers c and in particular for $c=y$. Hence there exists an integer m such that

$$mx \equiv y \bmod p \Rightarrow x^2+(mx)^2 \equiv x^2+y^2 \equiv 0 \bmod p.$$

Therefore $p|x^2(m^2+1)$ and since $p \nmid x$ it follows that $p|(m^2+1)$. That is $m^2 \equiv -1 \bmod p$. Equivalently -1 is a quadratic residue modulo a prime p of the form $4k+3$ which is impossible what we showed in the proof of Euler's theorem. This concludes the proof of the lemma. □

Lemma 2.16. *If p is a prime $p \equiv 3$ mod 4 and c is an odd integer such that $p^c|n$ but $p^{c+1} \nmid n$ then n cannot be represented as a sum of two squares.*

Proof. Assume

$$n=x^2+y^2, ggT(x,y)=d \Rightarrow x=dX, y=dY, ggT(X,Y)=1 \text{ with } n=d^2(X^2+Y^2)=d^2N.$$

Let p^r be the highest power of p which divides d. $\Rightarrow p^{c-2r}$ is the highest power of p dividing N with $c-2r>0$ since c is odd. $\Rightarrow N=X^2+Y^2, ggT(X,Y)=1$ and $p|N$ where $p \equiv 3 \bmod 4$. This contradicts the previous Lemma and hence it concludes the proof. □

Proof of the Theorem. 1. The condition is necessary: The second Lemma implies that if n is a sum of two squares, then every prime factor of n of the form $4k+3$ has an even exponent in the standard form of n.

2. The condition is sufficient: If n is a positive integer such that every prime factor of the form $4k+3$ which occurs in its standard form has an even exponent then n can be written as $n=n_1^2n_2$, where n_2 has no prime factors of the form $4k+3$. Therefore the only prime factors of n_2 are either the number 2 or odd primes of the form $4k+1$. Now 2 is representable as a sum of two squares 1^2+1^2 and every odd prime of the form $4k+1$ can be represented as a sum of two squares. Further the identity

$$(x_1^2+y_1^2)(x_2^2+y_2^2)=(x_1x_2+y_1y_2)^2+(x_1y_2-x_2y_1)^2$$

shows that the product of two numbers each of which is representable as a sum of two squares is likewise representable. Hence $n_2=a^2+b^2$, which implies that $n=(n_1a)^2+(n_1b)^2$. □

2.4 Sum of four squares

Theorem 2.17 (Lagrange's theorem)**.** *Every positive integer n is a sum of four squares.*

Theorem of Lagrange. Since $1=1^2+0^2+0^2+0^2$ we suppose in n what follows that $n>1$. The identity

$$(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)=z_1^2+z_2^2+z_3^2+z_4^2$$

where

$$z_1=x_1y_1+x_2y_2+x_3y_3+x_4y_4$$

$$z_2=x_1y_2-x_2y_1+x_3y_4-x_4y_3$$

$$z_3=x_1y_3-x_3y_1+x_4y_2-x_2y_4$$

$$z_4=x_1y_4-x_4y_1+x_2y_3-x_3y_2$$

shows that a product of two integers, each of which is representable as a sum of four squares is likewise representable. Every integer $n>1$ is a product of primes, and $2=1^2+1^2+0^2+0^2$. It suffices therefore to show that every odd prime is representable as a sum of four squares. It

follows from a previous Theorem (p odd prime $\Rightarrow \exists x, y$ s.t. $1 + x^2 + y^2 = mp, 0 < m < p$) that if p is an odd prime, then there exists an integer $m < p$ such that

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \text{ with } p \nmid x_1, x_2, x_3, x_4.$$

Given any odd prime p, let m_0 denote the smallest positive integer such that

$$m_0 p = x_1^2 + x_2^2 + x_3^2 + x_4^2, m_0 < p. \quad (4)$$

If $m_0 = 1$ there is nothing more to prove.

So suppose that $m_0 > 1$.

Step 1: Show that m_0 must be odd. Assume m_0 is even $\Rightarrow m_0 p$ is even too. Then x_1, x_2, x_3, x_4 are either all even, or all odd, or two even and two odd. Since

$$\frac{m_0 p}{2} = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2$$

we see that $m_0 p/2$ is a sum of four integer squares, not all of which are divisible by p. But this contradicts the minimality of m_0.

Hence $m_0 \geq 3$ and we can write

$$x_i = b_i m_0 + y_i \text{ for } i = 1, 2, 3, 4 \quad (5)$$

where the integer b_i can be so chosen that $|y_i| < m_0/2$.

For if the division of x_i by the odd number m_0 gives $x_i = b_i' m_0 + y_i'$ where $y_i' > m_0/2$ then we can write $x_i = (b_i' + 1)m_0 + (y_i' - m_0) = b_i m_0 + y_i$ where $-m_0/2 < y_i < 0$.

Now x_1, x_2, x_3, x_4 are not all divisible by m_0 because otherwise $m_0 | p$ which is impossible since $1 < m_0 < p$. Therefore $y_1^2 + y_2^2 + y_3^2 + y_4^2 > 0$. Thus we have

$$0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4(m_0/2)^2 = m_0^2$$

But if follows from (4) and (5) that $y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \bmod m_0$. Thus we have integers x_i, y_i for $i = 1, 2, 3, 4$ such that

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0 p, m_0 < p,$$

and

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_1 m_0, 0 < m_1 < m_0.$$

We have shown above, that products of sum of four squares are sum of four squares as well. Therefore we have

$$z_1, z_2, z_3, z_4 \text{ such that } z_1^2 + z_2^2 + z_3^2 + z_4^2 = m_0^2 m_1 p. \quad (6)$$

But

$$z_1 = \sum_{i=1}^{4} x_i y_i = \sum_{i=1}^{4} x_i(x_i - b_i m_0) \equiv \sum_{i=1}^{4} x_i^2 \bmod m_0 \equiv 0 \bmod m_0.$$

Similarly

$$z_2 \equiv z_3 \equiv z_4 \equiv 0 \bmod m_0.$$

Hence $z_i = m_0 t_i$, where t_i is an integer for $i = 1, 2, 3, 4$. On substituting these values in (6), we get

$$m_1 p = t_1^2 + t_2^2 + t_3^2 + t_4^2 \text{ with } 0 < m_1 < m_0.$$

But this contradicts the minimality of m_0. Hence $m_0 = 1$, and we conclude the proof. □

3 Representation of a natural number as the sum of eight squares

The aim of this second lesson is to find the number of representations of a natural number as a sum of eight squares by purely function theoretical means. This result is known as Jacobi's eight square-formula and goes as follows:

Theorem 3.1. *Let k, n be natural numbers and let*

$$A_k(n) := \#\{x = (x_1, \ldots, x_k) \in \mathbb{Z}^k \mid x_1^2 + \ldots + x_k^2 = n\}$$

be the number of ways one can represent n as a sum of k squares of integers. Then

$$A_8(n) = 16 \sum_{\substack{d|n \\ 1 \leq d \leq n}} (-1)^{n-d} d^3.$$

We use the following notation $z = x + iy \in \mathbb{C}$ and $q = e^{2\pi i z}$

In order to proof this formula we firstly introduce the theta series:

Proposition 3.2. *The function $\vartheta : \mathbb{H} \to \mathbb{C}$,*

$$\vartheta(z) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 z}.$$

represents an analytic function.

Now notice the following

$$\begin{aligned} \vartheta^k &= \left(\sum_{m_1 \in \mathbb{Z}} e^{\pi i m_1^2 z} \right) \cdot \ldots \cdot \left(\sum_{m_k \in \mathbb{Z}} e^{\pi i m_k^2 z} \right) \\ &= \sum_{m_1 \in \mathbb{Z}} \cdots \sum_{m_k \in \mathbb{Z}} e^{\pi i (m_1^2 + \ldots + m_k^2) z} \\ &= \sum_{n=0}^{\infty} A_k(n) e^{\pi i n z}. \end{aligned}$$

where $A_k(n)$ is as defined above. Thus we see that the Fourier coefficients of the k-th Power of the theta series are the desired values $A_k(n)$.

Secondly we look at the Eisenstein series:

Proposition 3.3. *The Eisenstein series of "weight" $k \geq 3$*

$$G_k(z) = \sum_{\substack{(c,d) \in \mathbb{Z}^2 \\ (c,d) \neq (0,0)}} \frac{1}{(cz + d)^k}$$

defines an analytic function on the upper half-plane. It is periodic with period 1 and for even $k \geq 4$ we have

$$\lim_{y \to \infty} G_k(z) = 2\zeta(k) = 2 \sum_{n=1}^{\infty} n^{-k}.$$

Moreover if k is odd the series identically vanishes.

We will need the following Lemma:

Lemma 3.4.

$$G_k\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right) = (\gamma z+\delta)^k G_k(z) \quad \textit{for} \quad \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}).$$

Proof. A small calculation shows

$$c\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right) + d = \frac{c'z+d'}{\gamma z+\delta}$$

with $c' = \alpha c + \gamma d$, $d' = \beta c + \delta d$.

As well as (c,d), the pair (c',d') runs through the set $\mathbb{Z}\times\mathbb{Z}\setminus(0,0)$. Thus

$$G_k\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right) = \sum_{(c,d)\neq(0,0)} \frac{1}{\left(c\frac{\alpha z+\beta}{\gamma z+\delta}+d\right)^k} = \sum_{(c',d')\neq 0} \frac{(\gamma z+\delta)^k}{(c'z+d')^k} = (\gamma z+\delta)^k G_k(z).$$

□

Proof of Proposition 3.3. For the convergence and analyticity see Lemma V.2.1 and V.8.1 in the book.

The periodicity $G_k(z+1) = G_k(z)$ directly follows from Lemma 3.4 since $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} z = z+1$.

Now because of the 1-periodicity of $G_k(z)$ it is enough to take the limit in the domain $|x| \leq \frac{1}{2}, y \geq 1$. In this region the Eisenstein series converges uniformly, so we can take the limit termwise. Obviously

$$\lim_{y\to\infty} (cz+d)^{-1} = 0 \quad \text{for} \quad c \neq 0.$$

This implies

$$\lim_{y\to\infty} G_k(z) = \sum_{d\neq 0} d^{-k} = 2\sum_{d=1}^{\infty} d^{-k} = 2\zeta(k).$$

Lastly if k is odd, then the terms (c,d) and $(-c,-d)$ cancel each other and thus the series vanishes. □

As the Eisenstein series is periodic we can look at its Fourier series

Proposition 3.5. *For any even $k \geq 4$ we have:*

$$G_k(z) = 2\zeta(k) + \frac{2\cdot(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n.$$

where

$$\sigma_k(n) := \sum_{\substack{d|n\\ 1\leq d\leq n}} d^k.$$

for $n \in \mathbb{N}$. In particular

$$G_4(z) = 2\frac{\pi^4}{90} + \frac{16}{3}\pi^4\sum_{n=1}^{\infty}\sigma_3(n)q^n.$$

All involved series are normally convergent in $\mathbb{H}$.

To proof this result we need the following Lemma and Corollary

Lemma 3.6. *Let* $\operatorname{Im} z > 0$*, then we have*

$$\sum_{n\in\mathbb{Z}} \frac{1}{(z+n)^2} = (2\pi i)^2 \sum_{n=1}^{\infty} n q^n.$$

Proof. We recall the partial fraction series decomposition of the cotangent and the negative of its derivative

$$\pi \cot(\pi z) = \frac{1}{z} + \sum_{n=1}^{\infty} \left[\frac{1}{z+n} + \frac{1}{z-n}\right]$$
$$\frac{\pi^2}{\sin^2(\pi z)} = \sum_{n=-\infty}^{\infty} \frac{1}{(z+n)^2}.$$

Both of these series converge normally in $\mathbb{C} \setminus \mathbb{Z}$ are 1-periodic and represent analytic functions in the upper half-plane. Thus they admit Fourier expansions.

One has

$$\pi \cot(\pi z) = \pi \frac{\cos(\pi z)}{\sin(\pi z)} = \pi i \frac{q+1}{q-1} = \pi i - \frac{2\pi i}{1-q} = \pi i - 2\pi i \sum_{n=0}^{\infty} q^n.$$

Differentiating with respect to z we obtain

$$\frac{\pi^2}{\sin^2(\pi z)} = (2\pi i)^2 \sum_{n=1}^{\infty} n q^n$$

and the claim follows. □

By taking repeated derivatives with respect to z, we obtain:

Corollary 3.7. *For any natural number* $k \geq 2$ *we have*

$$(-1)^k \sum_{n\in\mathbb{Z}} \frac{1}{(z+n)^k} = \frac{1}{(k-1)!} (2\pi i)^k \sum_{n=1}^{\infty} n^{k-1} q^n.$$

Proof of the Proposition. We rewrite the Eisenstein series

$$G_k(z) = \sum_{(c,d)\neq(0,0)} \frac{1}{(cz+d)^k} \quad (k \geq 4, k \equiv 0 \mod 2)$$

as

$$G_k(z) = 2\zeta(k) + 2 \sum_{c=1}^{\infty} \left\{ \sum_{d=-\infty}^{\infty} \frac{1}{(cz+d)^k} \right\}.$$

By Corollary 3.7, we have (after replacing z by cz and n by d)

$$G_k(z) = 2\zeta(k) + \frac{2(2\pi i)^k}{(k-1)!} \sum_{c=1}^{\infty} \sum_{d=1}^{\infty} d^{k-1} q^{cd}.$$

We now claim, that the series

$$\sum_{c=1}^{\infty} \sum_{d=1}^{\infty} d^{k-1} q^{cd} \qquad (|q| < 1)$$

converges normally in $\mathbb{H}$ for $k \geq 2$. First we rearrange the series, such that all terms with the

same q-exponent cd are grouped together. We obtain the series

$$\sum_{n=1}^{\infty} \left\{ \sum_{\substack{d|n \\ 1\leq d\leq n}} d^{k-1} \right\} q^n,$$

which converges for $|q| < 1$ due to the trivial estimate

$$\sum_{\substack{d|n \\ 1\leq d\leq n}} d^{k-1} \leq n \cdot n^{k-1} = n^k.$$

The above rearrangement can also be done with $|q|$ instead of q. This show the claimed normal convergence.

Moreover, the same rearrangements show, that the series Eisenstein Series $G_k(z)$ itself converges for all $k \geq 2$.

□

If we now look at Jacobi's Formula $A_8(n) = 16 \sum_{d|n} (-1)^{n-d} d^3$ we know that the left side are the Fourier coefficients of ϑ^8. And the right hand side is similar to the Fourier coefficients of $G_4(z)$ as both contain a sum of the type $\sum_{d|n} d^3$ up to some complications. This suggests that we might have to find a relation between ϑ^8 and G_4.

This is indeed the case and the proof is based on the following function theoretical characteristic of ϑ.

Remark 3.8. The theta series $\vartheta(z)$ has the following properties:

(a) $\vartheta(z+2) = \vartheta(z), \qquad \vartheta\left(-\frac{1}{z}\right) = \sqrt{\frac{z}{i}}\vartheta(z)$

(b) $\lim_{y\to\infty} \vartheta(z) = 1$

(c) $\lim_{y\to\infty} \sqrt{\frac{z}{i}}^{-1} \vartheta\left(1 - \frac{1}{z}\right) e^{-\frac{\pi i z}{4}} = 2$

where the square root of $\sqrt{\frac{z}{i}}$ is defined by using the principal branch of the logarithm.

For this result we need Jacobi's Theta Transformation Formula. Here without proof:

Theorem 3.9 (Jacobi's Theta Transformation Formula)**.** *For $(z, w) \in \mathbb{H} \times \mathbb{C}$ the following formula holds:*

$$\sqrt{\frac{z}{i}} \sum_{n=-\infty}^{\infty} e^{\pi i (n+w)^2 z} = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 (-1/z) + 2\pi i n w}.$$

Proof of Remark 3.8. The periodicity follows trivially:

$$\vartheta(z+2) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 (z+2)} = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 z} e^{2\pi i n^2} = \vartheta(z).$$

The second identity in (a) is a direct consequence of Theorem 3.9:

$$\vartheta\left(-\frac{1}{z}\right) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 (-1/z) + 2\pi i n \cdot 0} = \sqrt{\frac{z}{i}} \sum_{n=-\infty}^{\infty} \sum_{n=-\infty}^{\infty} e^{\pi i (n+0)^2 z} = \sqrt{\frac{z}{i}} \vartheta(z).$$

Due to the uniform convergence of the theta series we can take the limit in (b) termwise and get

$$\lim_{y\to\infty} \vartheta(z) = \lim_{y\to\infty} \sum_{n=-\infty}^{\infty} e^{\pi i n^2 (x+iy)} = \sum_{n=-\infty}^{\infty} \lim_{y\to\infty} e^{\pi i n^2 x} \cdot e^{-\pi n^2 y} = 1.$$

as for $n \neq 0$ the limit goes to 0 and for $n = 0$ to 1.

Lastly from Theorem 3.9 we also get the following identity:

$$\vartheta\left(1 - \frac{1}{z}\right) = \sqrt{\frac{z}{i}} \sum_{n=-\infty}^{\infty} e^{\pi i z(n+\frac{1}{2})^2}$$

and by applying it to the limit in (c) we get

$$\lim_{y\to\infty} \sqrt{\frac{z}{i}}^{-1} \vartheta\left(1 - \frac{1}{z}\right) e^{-\frac{\pi i z}{4}} = \sum_{n=-\infty}^{\infty} e^{\pi i z(n^2+n)} = 2.$$

by the same argument as above as for $n = -1$ and $n = 0$ the termwise limit is 1 and else 0. □

Proposition 3.10. *Let $r \in \mathbb{Z}$, and let $f : \mathbb{H} \to \mathbb{C}$ be an analytic function with properties:*

(a) $f(z+2) = f(z), \qquad f\left(-\frac{1}{z}\right) = \sqrt{\frac{z}{i}}^{r} f(z)$

(b) $\lim_{y\to\infty} f(z)$ *exists,*

(c) $\lim_{y\to\infty} \sqrt{\frac{z}{i}}^{-r} f\left(1 - \frac{1}{z}\right) e^{-\frac{\pi i r z}{4}}$ *exists.*

Then

$$f(z) = c \cdot \vartheta(z)^r$$

where $c = \lim_{y\to\infty} f(z)$.

For the proof of Proposition 3.10 see [FB] page 389f.

If we look at the Eisenstein Series however we find that G_4 doesn't satisfy the existence of the last limit. How ever the combination of $G_4(z)$ and $G_4(\frac{z+1}{2})$ yields the following

Proposition 3.11. *The function $f : \mathbb{H} \to \mathbb{C}$ given by*

$$f(z) = \frac{3}{\pi^4}\left(16G_4(z) - G_4\left(\frac{z+1}{2}\right)\right).$$

Satisfies all properties in Proposition 3.10 and has $\lim_{y\to\infty} f(z) = 1$. Thus

$$\vartheta(z)^8 = f(z).$$

Proof. Property (a) : As $G_4(z)$ is periodic with period 1 it follows that $G_4\left(\frac{z+1}{2}\right)$ is periodic with period 2 and therefore $f(z)$ also has period 2.

By using the notation from Lemma 3.4 we have

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} z = -\frac{1}{z} \quad \text{and} \quad \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix} \left(\frac{z+1}{2}\right) = \frac{-\frac{1}{z}+1}{2}.$$

and applying the same (Lemma 3.4) yields

$$G_4\left(-\frac{1}{z}\right) = z^4 G_4(z) \quad \text{and} \quad G_4\left(\frac{-\frac{1}{z}+1}{2}\right) = z^4 G_4\left(\frac{z+1}{2}\right)$$

and thus $f(-\frac{1}{z}) = \sqrt{\frac{z}{i}}^{8} f(z)$.

Property (b): We recall that $\lim_{y\to\infty} G_4(z) = 2\zeta(4) = 2 \cdot \frac{\pi^4}{90}$ and hence the limit in (b) exists

and equals

$$\lim_{y\to\infty} f(z) = \lim_{y\to\infty} \frac{3}{\pi^4}\left(16G_4(z) - G_4\left(\frac{z+1}{2}\right)\right) = \frac{3}{\pi^4}\cdot(16-1)\cdot 2\cdot\frac{\pi^4}{90} = 1.$$

Property (c) : As $G_4(z)$ is 1 periodic we have

$$G_4\left(1-\frac{1}{z}\right) = G_4\left(-\frac{1}{z}\right) = z^4 G_4(z) \quad \text{and} \quad G_4\left(\frac{(1-\frac{1}{z})-1}{2}\right) = G_4\left(-\frac{1}{2z}\right) = (2z)^4 G_4(2z)$$

and therefore

$$z^{-4} f\left(1-\frac{1}{z}\right) e^{-2\pi i z} = e^{-2\pi i z}\cdot\left(16G_4(z) - 16G_4(2z)\right).$$

From the Fourier series of G_4 we know that G_4 is a power series in q

$$G_4(z) = a_0 + a_1 q + a_2 q^2 + \dots$$

which implies that

$$z^{-4} f\left(1-\frac{1}{z}\right) e^{-2\pi i z} = q^{-1}\left[a_0(16-16) + \text{ higher } q\text{-powers}\right].$$

as the a_0 term is zero the factor q^{-1} gets absorbed by the higher q-powers and since

$$y \to \infty \Leftrightarrow q \to 0$$

we get the existence of the limit in (c).

Consequently we have shown that f satisfies all properties in Proposition 3.10 and thus $f(z) = c\cdot\vartheta(z)^r$ for $r = 8$. Moreover, as $\lim_{y\to\infty} f(z) = 1$ we have $c = 1$ and therefore $f(z) = \vartheta^8(z)$. $\square$

This is the final step in the puzzle. If we now compare the Fourier expansion of ϑ^8 and f we find

$$1 + \sum_{n=1}^{\infty} A_8(n) e^{\pi i n z} = 1 + 16^2 \sum_{n=1}^{\infty} \sigma_3(n) e^{2\pi i n z} - 16\sum_{n=1}^{\infty}\sigma_3(n)(-1)^n e^{\pi i n z}.$$

By writing $n = 2^t m$ with m odd and through comparing coefficients we get

$$\begin{aligned} A_8(n) &= 16^2 - \sigma_3\left(\frac{2^t m}{2}\right) - 16\sigma_3(2^t m) \\ &= 16^2 \sum_{d|2^{t-1}m} d^3 - 16 \sum_{d|2^{t-1}m} d^3. \end{aligned}$$

Now we collect all powers of 2 together which have the same divisor of m

$$\begin{aligned} A_8(n) &= 16^2 \sum_{d|m} (d^3 + (2d)^3 + \dots + (2^{t-1}d)^3) - 16\sum_{d|m}(d^3 + (2d)^3 + \dots + (2^t d)^3) \\ &= 2\cdot 16 \sum_{d|m}((2d)^3 + (2^2 d)^3 + \dots + (2^t d)^3) - 16\sum_{d|m}(d^3 + (2d)^3 + \dots + (2^t d)^3) \\ &= 16\sum_{d|m}(-1)^{n-d} d^3. \end{aligned}$$

where in the last step we used that the only divisors of $n = 2^t m$ that get a minus sign are the odd ones.

Thus we have shown the desired result

$$A_8(n) = \sum_{\substack{d|n \\ 1\leq d\leq n}} (-1)^{n-d} d^3.$$

References

[C] K. Chandrasekharan (1968) *Introduction to Analytic Number Theory*, Springer-Verlag New York

[FB] E. Freitag, R. Busam (2009) *Complex Analysis*, Springer-Verlag Berlin Heidelberg, 2nd ed.