SUMS OF SQUARES

JOSHUA BOSSHARDT

Abstract. This paper develops the structure of the multiplicative groups of units and quadratic residues for prime moduli to the end of investigating the representability of positive integers as sums of squares. It is shown that while some numbers can be written as a sum of two squares, all can be written as a sum of four squares.

Contents

1. Introduction

Beginning with an orientation in modular arithmetic, this paper first examines the collection of units for a given modulus as a multiplicative group, culminating in a demonstration of the cyclic structure of the unit group for prime moduli. This segues into an investigation of the group of quadratic residues, directed in particular towards determining for which primes is -1 a quadratic residue. With all the requisite tools developed, it ends by demonstrating which integers can be written as a sum of two squares while concluding that all can be written as a sum of four squares.

2. The Algebraic Structure of the Unit Group U_p

We begin constructing the basics of modular arithmetic.

Definition 2.1. If n is a positive integer and a and b are integers, we say that a and b are congruent modulo n if n divides $a - b$. We denote congruence modulo n by $a \equiv b \mod n$.

Theorem 2.2. *Congruence* $\bmod n$ *is an equivalence relation on* $\mathbb{Z}$.

Proof. Since $n \mid (a-a) = 0$ for all n, it follows $a \equiv a$. If $a \equiv b$, then $n \mid (a-b)$, which implies $n \mid (b-a)$. Therefore $b \equiv a$. If $a \equiv b$ and $b \equiv c$, then $n \mid (a-b)+(b-c) = (a-c)$, which means $a \equiv c$.

□

Date: August 30th, 2010.

The congruence relation thereby partitions $\mathbb{Z}$ into n equivalence classes, and we denote by $\mathbb{Z}_n$ the set of these equivalence classes. Denoting $[a]$ as the congruence class containing the integer a, we define $[a]+[b]=[a+b]$ and $[a][b]=[ab]$.

Theorem 2.3. *The additive and multiplicative operations on $\mathbb{Z}_n$ are well-defined.*

Proof. Let a and $a' \in [a]$ and b and $b' \in [b]$. Then there exist integers y and z such that $a-a'=ny$ and $b-b'=nz$. Thus $a+b-(a'+b')=n(y+z)$, and hence $a+b \equiv a'+b'$. Also, $ab-a'b'=n(nzy+a'z+b'y)$, so $ab \equiv a'b'$. □

I will henceforth abbreviate references to equivalence classes by omitting brackets around a representative element except when otherwise ambiguous. While it is obvious $\mathbb{Z}_n$ is closed under addition, subtraction, and multiplication, it remains unclear when an element possesses a multiplicative inverse. To answer this question, the following proof invokes Bezout's identity, which states that if $gcd(a,b)=d$ then there exist integers x and y such that $ax+by=d$. This is easily proven from the division algorithm.

Lemma 2.4. *If $gcd(a,b)=d$ then d is the least positive integer for which there exist integers x and y such that $ax+by=d$.*

Proof. Let $e=df$. If $gcd(a,b)=d$, then there exist integers x and y such that $ax+by=d$, which implies $axf+bxf=df=e$. Conversely, if there exist x and y such that $ax+by=c$, then since $d \mid a$ and $d \mid b$, it follows that $d \mid c$. Thus $ax+by=c$ if and only if $d \mid c$. Since d is the least positive multiple of d, the conclusion follows. □

Theorem 2.5. *An element $a \in \mathbb{Z}_n$ has a multiplicative inverse if and only if* $\gcd(a,n)=1$.

Proof. By Lemma 2.4, there exist integers x and y such that $ax+ny=1$ if and only if $\gcd(a,n)=1$. Thus, $ax \equiv 1 \bmod n$, which means $x \equiv a^{-1}$. □

Definition 2.6. If an element in $\mathbb{Z}_n$ has an inverse, we call it a *unit*. We denote the set of units in $\mathbb{Z}_n$ as U_n.

It follows from Theorem 2.5 that the set of units in $\mathbb{Z}_n$ forms a group under multiplication. Noting that the order of a group G, denoted by $|G|$, is the number of elements in G, observe that when the modulus is a prime p, $(U_p,\cdot)$ is a group of order $p-1$, since every integer less than p other than 0 is coprime to p.

The group structure of U_p gives rise to a useful identity in modular exponentiation we will later refer back to called Fermat's Little Theorem. In order to prove Fermat's Little Theorem we first prove Lagrange's Theorem.

Definition 2.7. The order of an element x in a group is defined as the smallest integer n such that $x^n=1$. If there is no such n, we say the order is infinity.

Lemma 2.8. *Let $x \in U_p$. If the order of x is n, then x^0, x^1, ..., x^{n-1} are distinct.*

Proof. Suppose there exist k and r where $0 \le r < k < n$ such that $x^k = x^r$. Then $x^{k-r}=1$. Since $k-r<n$, this contradicts the minimality of n. □

Definition 2.9. If G is a group with subgroup H and element x, then we say the left coset of H generated by x is the subset $\{xh \mid h \in H\}$, denoted more conveniently by xH.

Theorem 2.10. *(Lagrange's Theorem) If x is an element of the group G, then the order of x divides the order of G.*

Proof. Let H be the subgroup generated by x. By Lemma 2.8, the order of this subgroup is the same as the order of x. First we show that every element of G belongs to a unique left coset of H. Suppose there exists an element $y \in G$ that belongs to two cosets z_1H and z_2H. Then there exist h_1 and h_2 such that $z_1h_1 = y = z_2h_2$. We then have $z_1h_1h_2^{-1} = z_2$, implying $z_2H = z_1H$, which is a contradiction; thus, the left coset of any element of G is unique.

Also, every element of G is in a left coset of H since the map $f : G \to G$ defined by $f(x) = xh$ for a given fixed $h \in H$ is easily shown to be a bijection: since h^{-1} exists in the group, $xh = x'h$ implies $x = x'$, and since the domain and codomain are finite and have the same cardinality, the injectivity of f implies surjectivity and, consequently, bijectivity. Thus the left cosets of H partition G.

Now, the left cosets of H all contain $|H|$ elements. To prove this, suppose for a contradiction that the left coset generated by an element z contained less than $|H|$ elements. Then for some distinct h_1 and $h_2 \in H$ we have $zh_1 = zh_2$, which means $zh_1(h_2)^{-1} = z$. Since this is only true if $h_1 = h_2$, a contradiction results. Thus, if we denote the number of left cosets of H by $|G : H|$, then $|G| = |H| \cdot |G : H|$, which proves that the order of x divides the order of G. $\square$

Theorem 2.11. *(Fermat's Little Theorem) Let $a \in U_p$. Then $a^{p-1} \equiv 1 \bmod p$.*

Proof. Let n be the order of $x \in U_p$. By Lagrange's Theorem (Theorem 2.10), the order of an element of any group divides the order of the group. As a result, we have $n \mid p-1$. Let $r = \frac{p-1}{n}$. Then we get $a^{p-1} \equiv (a^n)^r \equiv 1^r \equiv 1 \bmod p$. $\square$

It follows that if the order of x in U_p is equal to $p-1$, then x generates the entire group of $p-1$ elements. We say that a group is *cyclic* if it contains such an element. In order to understand the structure of the quadratic residues of U_p, we now work towards proving that the group U_p is cyclic.

A useful arithmetic function for studying the organization of the unit group is the Euler totient function $\phi(n)$.

Definition 2.12. The Euler function $\phi(n)$ is defined to be the number of positive integers a less than n such that $\gcd(a, n) = 1$.

In particular, $\phi(n)$ specifices the number of elements in the group U_n. We now work towards developing a formula for $\phi(n)$.

Theorem 2.13. *Let p^k be a power of a prime p. Then $\phi(p^k) = p^k - p^{k-1}$.*

Proof. Since p is prime, an integer $a \in \mathbb{Z}_{p^k} \setminus \{0\}$ is coprime to p^k unless $p \mid a$. Thus every a is a unit except for multiples of p, of which there are p^{k-1}. $\square$

Theorem 2.14. *If a and b are coprime, then $\phi(ab) = \phi(a)\phi(b)$.*

Proof. We can list all the elements in $\mathbb{Z}_{ab}$ as follows:

$$\begin{array}{cccc} 1 & 2 & ... & a \\ a+1 & a+2 & ... & 2a \\ ... & ... & ... & ... \\ (b-1)a+1 & (b-1)a+2 & ... & ab \end{array}$$

It is clear that every column consists of integers which are congruent modulo a and that each row provides a complete set of residues of a.

Now, consider the map $f : \mathbb{Z}_b \to \mathbb{Z}_b$ defined by $f(r) = ra + c \bmod b$. If $ka + c \equiv k'a + c \bmod n$, then subtracting c and multiplying by a^{-1}, which exists since $\gcd(a, b) = 1$, we have $k \equiv k'$; since the domain and codomain are finite and have the same cardinality, the injectivity of the function implies surjectivity and thus bijectivity.

Thus, each column contains a complete set of residues of b. Since $\phi(a)$ is the number of columns whose congruence class is coprime to a and $\phi(b)$ is the number of rows whose congruence class is coprime to b, the number of integers coprime to ab is $\phi(a)\phi(b)$. □

Putting these two together, we arrive at an explicit enumeration of the totient function.

Theorem 2.15. *Let $n = p_1^{k_1} \cdot ... \cdot p_m^{k_m}$, where $p_1, ..., p_m$ are primes. Then $\phi(n) = \prod_{i=1}^{m}(p_i^{k_i} - p_i^{k_{i-1}})$.*

Proof. The proof is by induction on m. If $m = 1$, then by Theorem 2.13 the formula is true. Now, suppose by the inductive hypothesis that the theorem is true for m. Then if we take $n = p_1^{k_1}...p_{m+1}^{k_{m+1}}$, by Theorem 2.14 we have

$$\begin{aligned}
\phi(n) &= \phi(p_1^{k_1}...p_m^{k_m})\phi(p_{m+1}^{k_{m+1}}) \\
&= (\prod_{i=1}^{m} p_i^{k_i} - p_i^{k_{i-1}})(p_{m+1}^{k_{m+1}} - p_{m+1}^{k_m}) \\
&= \prod_{i=1}^{m+1} p_i^{k_i} - p_i^{k_{i-1}}.
\end{aligned}$$

□

The following corollary will be useful in the upcoming discussion on quadratic residues.

Corollary 2.16. *If $n > 2$, then $\phi(n)$ is even.*

Proof. From Theorem 2.15, we have $\phi(n) = \prod_{i=1}^{m}(p_i^{k_i} - p_i^{k_{i-1}})$. It follows from the well-definedness of modular multiplication that the parity of r is preserved under exponentiation. Also, since n is greater than 2 and the difference between two numbers of the same parity is even, at least one factor of $\phi(n)$ is even, rendering the entire product even. □

Having developed the Euler function, we continue to the theorems needed to prove that U_p is cyclic.

Theorem 2.17. *Let $f(x) = a_0 + a_1x + ... + a_nx^d$ be a polynomial of degree d over $\mathbb{Z}_p$ where $a_i \neq 0 \bmod p$ for some i. Then f has at most d roots.*

Proof. We prove this theorem by induction on d. If $d = 0$ then $f(x) = a_0$ where a_0 is not divisible by p; this equation has 0 roots, satisfying the desired conclusion. Now consider a polynomial f of degree d in which at least one coefficient is not divisible by p. If f has no roots, then we are done. If f has a root c, then

$$f(x)-f(c)=\sum_{i=1}^{d} a_i(x^i-a^i)=\sum_{i=1}^{d}(x-c)a_i(x^{i-1}+cx^{i-2}+...+c^{i-1})=(x-c)g(x),$$

where $g(x)$ is a polynomial of degree $d-1$. If all the coefficients of g are divisible by p, then $p \mid (x-c)g(x)+f(c)=f(x)$, which contradicts the fact that f has at least one coefficient not divisible by p. Thus by the inductive hypothesis suppose that g has at most $d-1$ roots. Let b be a root of f. Then $f(b) \equiv \bmod p$ if and only if $(b-c)g(b) \equiv 0$. Since g has at most $d-1$ roots, the maximum number of roots of f is $1+(d-1)=d$. $\square$

Theorem 2.18. *If $n \geq 1$, then $\sum_{d|n} \phi(d) = n$.*

Proof. Let $T_d = \{m \in \mathbb{Z}_n \mid m < n \text{ and } \gcd(m,n)=d\}$. It is clear that the sets T_d for every d dividing n partition $\mathbb{Z}_n$ since $\gcd(m,n)$ is unique for every m. It follows directly from Bezout's identity that if $\gcd(m,n)=d$, then $\gcd(\frac{m}{d},\frac{n}{d})=1$, which means if we let $R_d=\{m \mid m<n \text{ and } gcd(\frac{m}{d},\frac{n}{d})=1\}$, then $|R_d|=|T_d|$ and the sets R_d form a partition of $\mathbb{Z}_n$. Based on its definition, $|R_d|=\phi(\frac{n}{d})$. Thus $\sum_{d|n}\phi(\frac{n}{d})=n$. However, $\sum_{d|n}\phi(\frac{n}{d})=\sum_{d|n}\phi(d)$ since $\frac{n}{d}$ is a factor of n, which means $\sum_{d|n}\phi(d)=n$. $\square$

Theorem 2.19. *If p is prime, then U_p has $\phi(d)$ many elements of order d for each d dividing $p-1$.*

Proof. Let $T_d=\{r \in U_p \mid m \text{ has order } d\}$, where d is a factor of $p-1$. By Lagrange's Theorem (Theorem 2.10), the order of an element in U_p divides $p-1$, and since the order of an element is unique, the sets T_d for all d dividing $p-1$ partition U_p. Thus, $\sum_{d|n}|T_d|=p-1$. From Theorem 2.18, this implies $\sum_{d|n}(\phi(d)-|T_d|)=0$, which means if each term is nonnegative, or if $\phi(d)\geq|T_d|$ for all d, then $\phi(d)=|T_d|$.

Let $r \in T_d$. The set $R=\{r^i \mid i \in \mathbb{Z} \text{ such that } 0<i\leq d\}$ consists of d roots of the polynomial $f(x)=x^d-1$ in $\mathbb{Z}_p$. Since the coefficients are coprime to p, the polynomial has at most d roots by Theorem 2.17, which means R is a complete set of roots of f. As a result, if $m \in T_d$, then $m=r^k$ for some integer k. Let $\gcd(k,d)=y$. Then we have

$$m^{\frac{d}{y}}=r^{\frac{kd}{y}}=(r^d)^{\frac{k}{y}}=1^{\frac{k}{y}}=1.$$

Since d is the order of m, it follows that $y=1$. Thus every element $m \in T_d$ can be written as r^k for k such that $0<k\leq d$ and $\gcd(k,d)=1$, which means the number of such elements cannot exceed $\phi(d)$ for any d. Hence $\phi(d)-|T_d|$ is nonnegative for every d, which implies $|T_d|=\phi(d)$ for all d dividing $p-1$. $\square$

Theorem 2.20. *The group U_p is cyclic.*

Proof. By Theorem 2.19, U_p has $\phi(p-1)$ elements of order $p-1$. Since $\phi(p-1)\neq 0$ and $p-1$ is the order of the group, U_p is cyclic. $\square$

Example 2.21. Let $p=5$. Listing the powers of 2 mod 5 we have 2,4,3, and 1. Thus U_5 is a cyclic group in which 2 is a primitive root.

3. Determining Quadratic Residues of U_p

Definition 3.1. An element $a \in U_n$ is a quadratic residue of n if there exists $t \in U_n$ such that $t^2 \equiv a \bmod n$. Denote the set of quadratic residues as Q_n.

It is clear that Q_n forms a group under multiplication. We now work towards determining whether $-1 \in Q_p$ for a given odd prime p.

Theorem 3.2. *Let $n > 2$ and g be a primitive root for U_p. Then Q_p forms a cyclic group of order $\frac{\phi(n)}{2}$ generated by g^2.*

Proof. Let $a \in U_p$. Then there exists $i \in \mathbb{Z}$ such that $a = g^i$. If i is even, $g^i = (g^{\frac{i}{2}})^2$, which means $a \in Q_p$. Note also that $a = (g^2)^{(\frac{i}{2})}$ and is consequently a multiple of g^2. If $a \in Q_p$, then there exists $s \in U_p$ such that $a = s^2$, where $s = g^j$ for some integer j. This means $a = s^2 = (g^j)^2 = (g^2)^j$. Thus Q_p is the subgroup of U_p generated by g^2. Since $\phi(n)$ is even from Corollary 2.16, we have $(g^2)^{\frac{\phi(n)}{2}} \equiv 1$, which means g^2 generates a subgroup of order $\frac{\phi(n)}{2}$. □

It quickly follows from Theorem 3.2 that if $a = g^i$ for a primitive root g, then $a \in Q_p$ if and only if $i \equiv 0 \bmod 2$. We now develop a general formula, the Euler criterion, for determining whether an element is in Q_p.

Theorem 3.3. *If p is an odd prime and a is in U_p, then $a \in Q_p$ if and only if $a^{\frac{p-1}{2}} \equiv 1 \bmod p$.*

Proof. Let g be a primitive root of U_p. First consider $g^{\frac{p-1}{2}}$. Since $(g^{\frac{p-1}{2}})^2 \equiv 1$ by Fermat's Little Theorem (Theorem 2.11), we have $p \mid (g^{\frac{p-1}{2}} - 1)(g^{\frac{p-1}{2}} + 1)$, which implies one of the factors must be a multiple of p; this implies $g^{\frac{p-1}{2}} = \pm 1$. However, if $g^{\frac{p-1}{2}} \equiv 1$, this would contradict the fact that the order of g is $p-1$. Thus $g^{\frac{p-1}{2}} \equiv -1 \bmod p$ Let $a = g^i$. Then we have

$$a^{\frac{p-1}{2}} \equiv (g^i)^{\frac{p-1}{2}} \equiv (g^{\frac{p-1}{2}})^i \equiv (-1)^i.$$

Since $a \in Q_p$ if and only if $i \equiv 0 \bmod 2$, it follows that $a \in Q_p$ if and only if $a^{\frac{p-1}{2}} \equiv 1 \bmod p$. □

This brings us to the desired result.

Theorem 3.4. $-1 \in Q_p$ *if and only if* $p \equiv 1 \bmod 4$.

Proof. $(-1)^{\frac{p-1}{2}} \bmod p = (-1)^{\frac{p-1}{2}}$. From Theorem 3.3, $-1 \in Q_p$ if and only if $\frac{p-1}{2}$ is even, which is true if and only if $p \equiv 1 \bmod 4$. □

Having proven for which primes -1 is a quadratic residue, we have everything needed to determine which numbers can be written as a sum of two squares.

4. Sums of Two Squares

Definition 4.1. For each integer $k \geq 1$, denote $S_k = \{n \mid n = x_1^2 + ... + x_k^2$ for some $x_1, ..., x_k \in \mathbb{Z}\}$. This is the set of sums of k squares.

Lemma 4.2. S_2 *is closed under multiplication.*

Proof. Let a_1,b_1,a_2,$b_2 \in \mathbb{Z}$. The theorem follows immediately from the identity:

$$(a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1a_2 + b_1b_2)^2 + (a_1b_2 - a_2b_1)^2.$$

□

Theorem 4.3. *Each prime $p \equiv 1 \bmod 4$ is a sum of two squares.*

Proof. Since $p \equiv 1 \bmod 4$, we have $-1 \in Q_p$. Thus there exists $x \in U_p$ such that $x^2 \equiv -1$. It follows that $1 + x^2 = mp$, with $m \in \mathbb{Z}$. Since we can choose x such that $x \leq p - 1$, we have

$$1 + x^2 \leq 1 + (p-1)^2 \leq p^2 - 2p + 2 < p^2.$$

This means $0 < r < p$. Now, consider the set $R = \{r \in \mathbb{Z} \mid rp \in S_2\}$. By the Well-Ordering principle R has a least element t, where

$$tp = a_1^2 + b_1^2$$

with a_1,$b_1 \in \mathbb{Z}$. If $t = 1$, the theorem is already true, so assume $t > 1$. Choose a_2,$b_2 \in \mathbb{Z}$ such that $a_2 \equiv a_1 \bmod t$ and $b_2 \equiv b_1 \bmod t$, where a_2 and b_2 are the least absolute residues of a_1 and b_1 modulo t. Then there exists s such that

$$st = a_2^2 + b_2^2.$$

Given that a_2 and b_2 are the least absolute residues of t, we have

$$st = a_2^2 + b_2^2 \leq 2\left(\frac{t}{2}\right)^2 = \frac{t^2}{2} < t^2,$$

which implies $s < t$. We also know $s \neq 0$ since if $s = 0$ then $a_1, b_1 \equiv 0 \bmod t$, which means $t^2 \mid a_1^2 + b_1^2$. Since $a_1^2 + b_1^2 = tp$, we have $t \mid p$, contradicting the fact that p is prime and that $0 < t < p$. By Lemma 4.2,

$$pst^2 = (a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1a_2 + b_1b_2)^2 + (a_1b_2 - a_2b_1)^2.$$

If we can show that $a_1a_2 + b_1b_2$ and $a_1b_2 - a_2b_1$ are divisible by t, then

$$ps = \left(\frac{a_1a_2 + b_1b_2}{t}\right)^2 + \left(\frac{a_1b_2 - a_2b_1}{t}\right)^2.$$

Examining the two terms, we have the following:

$$\begin{aligned} a_1a_2 + b_1b_2 &\equiv a_1^2 + b_1^2 \equiv 0 \bmod t \\ a_1b_2 - a_2b_1 &\equiv a_1b_1 - a_1b_1 \equiv 0 \bmod t. \end{aligned}$$

Both terms are divisible by t and hence form a sum of two squares to a multiple of p less than t, contradicting the fact that t is the minimal element of R. Thus, $t = 1$, which completes the proof. □

We can generalize this result to arbitrary $n \in \mathbb{N}$.

Theorem 4.4. *Let $p_1, ..., p_k$ be primes congruent to 1 modulo 4 and $q_1, ..., q_r$ be primes congruent to 3 modulo 4. A positive integer n is a sum of squares if and only if n is of the form $n = 2^e(p_1^{e_1} \cdot ... \cdot p_k^{e_k})((q_1^2)^{f_1} \cdot ... \cdot (q_r^2)^{f_r})$, where $e_i, f_i \in \mathbb{Z}$.*

Proof. Since 2 is a sum of two squares, it is clear from the closure of S_2 (Lemma 4.2) that any n of the form $n = 2^e(p_1^{e_1} \cdot ... \cdot p_k^{e_k})((q_1^2)^{f_1} \cdot ... \cdot (q_r^2)^{f_r}$ is a sum of two squares.

Now suppose, for a contradiction, that there exists $n \in S_2$ divisible by q^{2f+1}, where $2f+1 \geq 0$ is the greatest integer power of q which divides n. Since $n \in S_2$, there exist x and y such that $n = x^2 + y^2$. Since $q^{2f+1} \mid n$, there exists $r \in \mathbb{Z}$ such that $x^2 + y^2 = q^f r$. Now, let $\gcd(x, y) = d$. Let e be the greatest power of q which divides d so that there exists $k \in \mathbb{Z}$ such that $q^e k = d$, which means $q^{2e}k^2 = d^2$. Then we have $\frac{q^{2f+1}r}{d^2} = q^{2(f-e)+1}\frac{r}{k^2} = \left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2$. Since $2(f-e)+1 \equiv 1 \bmod 2 \neq 0$ we have $q \mid \left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2$, which implies $\left(\frac{x}{d}\right)^2 \equiv -\left(\frac{y}{d}\right)^2 \bmod q$. If either $\frac{x}{d}$ or $\frac{y}{d}$ is congruent to 0 modulo q, then so is the other. Since $\gcd(\frac{x}{d}, \frac{y}{d}) = 1$, neither is congruent to 0. Consequently, $\frac{x}{d}, \frac{y}{d} \in U_q$, so there exists $\left(\frac{y}{d}\right)^{-1} \in U_q$. Thus $\left(\frac{x}{d}\right)^2 \equiv -\left(\frac{y}{d}\right)^2$ implies $(\frac{x}{d}\left(\frac{y}{d}\right)^{-1})^2 \equiv -1 \bmod q$, which by Theorem 3.4 contradicts the fact that q is congruent to 3 modulo 4. □

Example 4.5. Consider $n = 30$ and $m = 490$. It is easy to check that n is not a sum of two squares. The prime factorization of n gives $n = 2 \cdot 3 \cdot 5$, where $3 \equiv 3 \bmod 4$ and is raised to an odd power. However, the prime factorization of m is $m = 2 \cdot 5 \cdot 7^2$, where every prime congruent to 3 modulo 4 is raised to an even power, so we would expect to find that m is a sum of two squares. Lemma 4.2 provides the method for finding two integers whose sum of squares sums to 490. We first note $2 = 1^2 + 1^2$ and $5 = 1^2 + 2^2$, so Lemma 4.2 gives $2 \cdot 5 = (1+1)(1+2^2) = 3^2 + 1^2$. Applying the lemma again we have $(2 \cdot 5) \cdot 7^2 = (3^2+1)(7^2+0) = 21^2 + 7^2 = 490$.

5. Sums of Four Squares

The strategy of the proof for showing that any integer is a sum of four squares closely mirrors the earlier proof regarding sums of two squares. Hence we begin with a similar lemma.

Lemma 5.1. *S_4 is closed under multiplication.*

Proof. Let $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in \mathbb{Z}$. Then the following identity proves the theorem:

$$\begin{aligned}(a_1^2 + b_1^2 + c_1^2 + d_1^2)(a_2^2 + b_2^2 + c_2^2 + d_2^2) =&(a_1a_2 + b_1b_2 + c_1c_2 + d_1d_2)^2 + \\ &(a_1b_2 - b_1a_2 + c_1d_2 - c_2d_1)^2 + \\ &(a_1c_2 + b_1d_2 - a_2c_1 - b_2d_1)^2 + \\ &(a_1d_2 - d_1a_2 + c_1b_2 - c_2b_1)^2.\end{aligned}$$

□

Since 2 and any prime $p \equiv 1 \bmod 4$ is a sum of two non-zero squares and thus a sum of four squares, to prove that any positive integer n is a sum of four squares it suffices to show, by Lemma 5.1, that any prime q congruent to 3 modulo 4 is a sum of four squares.

Theorem 5.2. *Any prime $q \equiv 3 \bmod 4$ is a sum of four squares.*

Proof. First we need to show that a multiple of q is a sum of four squares. To this end, consider the following sets:

$$R = \{z \in \mathbb{Z}_q \mid z \equiv k^2, k \in U_q\}$$

$$S = \{y \in \mathbb{Z}_q \mid y \equiv -1 - r^2, r \in U_q\}.$$

From Theorem 3.2, Q_q contains $\frac{q-1}{2}$ elements, which means the total number of squares in $\mathbb{Z}_q$ is $\frac{q+1}{2}$, the cardinality of the set $Q_q \cup \{0\}$. Since $\frac{q+1}{2} > \frac{|\mathbb{Z}_q|}{2}$, we have $R \cap S \neq \emptyset$, which means there exists an element $z \in Q_q$ such that $z \equiv k^2 \equiv -1 - r^2$. This implies $k^2 + r^2 + 1 \equiv 0 \bmod q$, which means that a multiple of any prime is a sum of four squares. To generalize, we can say there exist a_1,b_1,c_1,$d_1 \in \mathbb{Z}$ such that $a_1^2 + a_2^2 + a_3^2 + a_4^2 = mp$, where $m \in \mathbb{Z}$. Choosing the least absolute residues for a_1,b_1,c_1,d_1 mod p, we have

$$mp = a_1^2 + b_1^2 + c_1^2 + d_1^2 \leq 4\left(\frac{p-1}{2}\right)^2 \leq (p-1)^2 < p^2,$$

which means $0 < m < p$. Consider the set $R = \{m \in \mathbb{Z}_q \mid mp \in S_4\}$. By the Well-Ordering principle R has a least element t, where

$$tp = a_1^2 + b_1 + c_1^2 + d_1^2$$

with a_1,b_1,c_1,$d_1 \in \mathbb{Z}$. If $t = 1$, the theorem is already true, so assume $t > 1$. Choose a_2,b_2,c_2,$d_2 \in \mathbb{Z}$ such that $a_2 \equiv a_1 \bmod t$ and $b_2 \equiv b_1 \bmod t$, $c_2 \equiv c_1 \bmod t$, and $d_2 \equiv d_1 \bmod t$, where a_2, b_2,c_2,d_2 are the least absolute residues of a_1,b_1,c_1,d_1 modulo t. Then there exists s such that

$$st = a_2^2 + b_2^2 + c_2^2 + d_2^2.$$

If t is odd, then since a_2, b_2, c_2, and d_2 are less than $\frac{t}{2}$, we have $st = a_2^2 + b_2^2 + c_2^2 + d_2^2 < 4\left(\frac{t}{2}\right)^2 = t^2$, which implies $s < t$. If t is even, however, then any given least absolute residue is less than or equal to $\frac{t}{2}$, which only implies $s \leq t$. However, suppose t is even. Then, since parity is preserved under exponentiation, out of a_2, b_2,c_2, and d_2 there must be two pairs of numbers with the same parity. Without loss of generality, assume a_2 and b_2 have the same parity and c_2 and d_2 have the same parity. Then

$$\left(\frac{a_2+b_2}{2}\right)^2 + \left(\frac{a_2-b_2}{2}\right)^2 + \left(\frac{c_2+d_2}{2}\right)^2 + \left(\frac{c_2-d_2}{2}\right)^2 = \left(\frac{a_2^2+b_2^2+c_2^2+d_2^2}{2}\right)^2 = \frac{tp}{2},$$

contradicting the minimality of t. Thus, $s < t$. Now, if $s = 0$ then, by a similar argument as Theorem 4.3, we would have $t \mid p$, contradicting the fact that p is prime and that $0 < t < p$. Consider

$$\begin{aligned} t^2 sp &= (a_2^2 + b_2^2 + c_2^2 + d_2^2)(a_1^2 + b_1^2 + c_1^2 + d_1^2) \\ &= (a_1a_2 + b_1b_2 + c_1c_2 + d_1d_2)^2 + (a_1b_2 - b_1a_2 + c_1d_2 - c_2d_1)^2 + \\ &\quad (a_1c_2 + b_1d_2 - a_2c_1 - b_2d_1)^2 + (a_1d_2 - d_1a_2 + c_1b_2 - c_2b_1)^2. \end{aligned}$$

Thus, if we show t divides each squared integer on the right hand side, then

$$\begin{aligned} sp = &\left(\frac{a_1a_2 + b_1b_2 + c_1c_2 + d_1d_2}{t}\right)^2 + \left(\frac{a_1b_2 - b_1a_2 + c_1d_2 - c_2d_1}{t}\right)^2 + \\ &\left(\frac{a_1c_2 + b_1d_2 - a_2c_1 - b_2d_1}{t}\right)^2 + \left(\frac{a_1d_2 - d_1a_2 + c_1b_2 - c_2b_1}{t}\right)^2. \end{aligned}$$

Analyzing each equation for its divisibility by t, we have:

$$\begin{aligned}
a_1a_2 + b_1b_2 + c_1c_2 + d_1d_2 &\equiv a_1^2 + b_1^2 + c_1^2 + d_1^2 \equiv 0 \bmod t \\
a_1b_2 - b_1a_2 + c_1d_2 - c_2d_1 &\equiv a_1b_1 - a_1b_1 + c_1d_1 - c_1d_1 \equiv 0 \bmod t \\
a_1c_2 + b_1d_2 - a_2c_1 - b_2d_1 &\equiv a_1c_1 + b_1d_1 - a_1c_1 - b_1d_1 \equiv 0 \bmod t \\
a_1d_2 - d_1a_2 + c_1b_2 - c_2b_1 &\equiv a_1d_1 - d_1a_1 + c_1b_1 - c_1b_1 \equiv 0 \bmod t.
\end{aligned}$$

Since $s < t$, this contradicts the minimality of t; therefore $t = 1$. Hence, any positive integer is representable as a sum of four squares. □

Example 5.3. While in Example 4.5 we showed that 30 is not representable as a sum of two squares, we now show that it is representable as a sum of four squares. Recall that the prime factorization of 30 is $30 = 2 \cdot 3 \cdot 5 = (1+1+0+0)(1+1+1+0)(2^2+1+0+0)$. Using Lemma 5.1, $(1+1+0+0)(1+1+1+0) = 2^2+0+1^2+(-1)^2$. Using the lemma again, $(2^2+1+1+0)(2^2+1+0+0) = 5^2+0+2^2+1^2 = 30$.

Acknowledgements

I would like to thank my mentor Daniele Rosso for assisting me in the production of this paper.

References

[1] Jones, Gareth A. Elementary Number Theory. London: Springer-Verlog; London, 1998.