$\mathbb{Z}[\omega], \mathbb{Z}[\sqrt[3]{2}]$, and Cubic Reciprocity

Gautham Anne

1 Units of $\mathbb{Z}[\sqrt[3]{2}]$

Of the form $\pm(\sqrt[3]{2}-1)^k$ for $k \in \mathbb{Z}$

$$N(a+b\sqrt[3]{2}+c\sqrt[3]{4}) =$$
$$(a+b\sqrt[3]{2}+c\sqrt[3]{4})(a+b\omega\sqrt[3]{2}+c\omega^2\sqrt[3]{4})(a+b\omega^2\sqrt[3]{2}+c\omega\sqrt[3]{2}) = a^3+2b^3+4c^3-6abc$$

2 Conjectures about $\mathbb{Z}[\omega]$

Theorem 2.1. *The Norm of $\mathbb{Z}[\omega]$ is a^2-ab+b^2.*

1. If α prime in $\mathbb{Z}[\omega]$, then N(α) $= p$ or p^2, where p is a rational prime. Moreover, if N(α) $= p^2$, then α and p are associates.
2. If N(α) prime in $\mathbb{Z}$, then α prime in $\mathbb{Z}[\omega]$.
3. If p, a rational prime, is congruent to 2 mod 3, then it is prime in $\mathbb{Z}[\omega]$.
4. Modding out $\mathbb{Z}[\omega]$ by a prime α will result in a field with N(α) elements.
5. If p is a rational prime congruent to 2 mod 3, then p is prime in $\mathbb{Z}[\omega]$.
6. If p is a rational prime congruent to 1 mod 3, then p $= \alpha\overline{\alpha}$ for prime α in $\mathbb{Z}[\omega]$.
7. **FLT? :** If α prime in $\mathbb{Z}[\omega]$, and $\alpha \nmid \pi$ then $\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$
8. $\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{(N(\alpha)-1)/3} \pmod{\pi}$
9. $\left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3 = \left(\frac{\alpha\beta}{\pi}\right)_3$
10. If $\alpha \equiv \beta \pmod{\pi}$, $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$
11. $\overline{\left(\frac{\alpha}{\pi}\right)_3} = \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_3$, where $\overline{\alpha}$ is the complex conjugate of α.

3 Small Theorems on Cubic Reciprocity

Define $\left(\frac{x}{p}\right)_3 = x^{\frac{p-1}{3}}$ to be the cubic Legendre symbol (for $p \equiv 1 \pmod 3$). Let $\left(\frac{x}{p}\right)_3 = 0$ if $p|x$.

Theorem 3.1. *$\left(\frac{x}{p}\right)_3$ must be one of 3 values if $p \equiv 1 \pmod 3$. Of the 3 values, one is 1, while for the other two, each is the square of the other. Also, the sum of the 3 possibilities is p.*

Proof. Since $\left(\left(\frac{x}{p}\right)_3\right)^3 = x^{p-1} \equiv 1 \pmod p$, the value of $\left(\frac{x}{p}\right)_3$, which will be abbreviated to a for the remainder of the proof, must satisfy $a^3 \equiv 1 \pmod p$. This means that $a^3 - 1 \equiv 0 \pmod p$, so $(a-1)(a^2+a+1) \equiv 0 \pmod p$. Since $\mathbb{Z}_p$ is a UFD and p is prime, either $a \equiv 1 \pmod p$ or $a^2 + a + 1 \equiv 0 \pmod p$, which means that there is a total of 3 residues that can work.

In addition, we can see that $0 \equiv a^2 + a + 1 \equiv a^2 + a^4 + 1$, so if a satisfies $a^2+a+1 \equiv 0 \pmod p$, so does a^2. We can also see that $\left(a^2\right)^2 = a^4 \equiv a \pmod p$ because $a^3 \equiv 1$, so for the two possible values that are not 1, each is the square of the other.

All residues lie between 0 to $p-1$, and since one of them is 1, the sum of the 3 is at most $p - 1 + p - 2 + 1 = 2p - 2$ and greater than 1. But since their sum is divisible by p, this means that the sum of the 3 possible values for $\left(\frac{x}{p}\right)_3$ always sums to p.

□

Theorem 3.2. *If $p \equiv 2 \pmod 3$, then every integer is a cubic residue modulo p.*

Proof. Let $p = 3n + 2$. By Fermat's little theorem, $x^{3n+1} \equiv 1 \pmod p$. Then $x \equiv x \cdot (x^{3n+1})^2 \equiv (x^{2n+1})^3 \pmod 3$, so, by construction, every integer is a cubic residue. □

Theorem 3.3. *If $p \equiv 1 \pmod 3$, then there exist unique $m, n, \in \mathbb{Z}^+$ such that $4p = m^2 + 27n^2$.*

We first begin with the following lemma:

Lemma 3.4. *If $p \equiv 1 \pmod 3$, then there exist $A, B \in \mathbb{Z}^+$ such that $p = A^2 + AB + B^2$.*

Proof. If $p \equiv 1 \pmod 3$, then $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}$ (by QR) and $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ (by Euler's criterion), so $\left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{-1}{p}\right) = (-1)^{p-1} = 1$. Thus the solutions to $x^2 + x + 1 = 0$, namely $x = \frac{-1\pm\sqrt{-3}}{2}$ exist in $\mathbb{Z}_p$. In other words, there exists x such that $x^2 + x + 1 \equiv 0 \pmod p$. Let this value of x be x'. Now consider the ring $\mathbb{Z}[\omega]$. Note that $p|x'^2 + x' + 1 = (x' - \omega)(x' - \omega^2)$. But

$p \nmid (x-\omega)$ and $p \nmid (x-\omega^2)$, so p is not prime in $\mathbb{Z}[\omega]$. It is now easy to see that $p = \alpha \cdot \overline{\alpha}$ for some $\alpha \in \mathbb{Z}[\omega]$. If $\alpha = a + b \cdot \frac{-1+\sqrt{-3}}{2}$, then $p = a^2 - ab + b^2$.

Now, if exactly one of a or b is negative (WLOG, say $a = A$, $-b = B$ with $A, B \in \mathbb{Z}^+$), then $p = A^2 + AB + B^2$, and we are done. The only other cases are when a and b share sign. Note that both of these cases (a and b positive or negative) are symmetric, so it suffices to prove one of these cases. WLOG let $a > b$. Consider $A = a - b$ and $B = b$. Then $A^2 + AB + B^2 = (a-b)^2 + (a-b)b + b^2 = a^2 - ab + b^2 = p$, so we are done.

The following can only be noted by the genius mind: $4p = 4A^2+4AB+4B^2 = (A+2B)^2 + 3A^2 = (2A+B)^2 + 3B^2 = (A-B)^2 + 3(A+B)^2$. If either A or B is a multiple of 3, then the theorem is true. If not, note that $A \not\equiv B \pmod 3$, because otherwise we would derive $p \equiv 0 \pmod 3$. Then $A + B \equiv 1 + 2 \equiv 0 \pmod 3$. Thus, given a solution (A, B) to $p = A^2 + AB + B^2$, we can construct a solution to $4p = m^2 + 27n^2$.

□

Theorem 3.5. *The solution $(m, n) \in \mathbb{Z}^+ \times \mathbb{Z}^+$ to $4p = m^2 + 27n^2$ is unique.*

Proof. Assume there are two distinct solutions $(a_1, b_1), (a_2, b_2)$. Then $a_1^2 + 27b_1^2 = a_2^2 + 27b_2^2 \Rightarrow 27 = \frac{a_2^2 - a_1^2}{b_1^2 - b_2^2}$. Substituting, $4p = a_1^2 + (27)b_1^2 = a_1^2 + \left(\frac{a_2^2-a_1^2}{b_1^2-b_2^2}\right) b_1^2 = \frac{a_2^2b_1^2 - a_1^2b_2^2}{b_1^2-b_2^2} = \frac{(a_2b_1-a_1b_2)(a_2b_1+a_1b_2)}{(b_1-b_2)(b_1+b_2)}$. We will achieve our contradiction by showing that $a_2b_1 + a_1b_2 < p$.

By Cauchy-Schwarz, $(a_1^2 + a_2^2)(b_2^2 + b_1^2) \geq (a_1b_2 + a_2b_1)^2$. But $a_1^2 + a_2^2 = (4p - 27b_1^2) + (4p - 27b_2^2) = 8p - 27(b_1^2 + b_2^2)$, so $(8p - 27(b_1^2 + b_2^2))(b_2^2 + b_1)^2 \geq (a_1b_2 + a_2b_1^2)$. It is well known that $max((a-x)x) = \frac{a^2}{4}$ for reals x and constant a, so $(8p - 27(b_1^2 + b_2^2))(b_2^2 + b_1^2) = 27 \cdot (\frac{8p}{27} - (b_2^2 + b_1^2))(b_2^2 + b_1^2) \leq 27 \cdot \left(\frac{4p}{27}\right)^2 = \frac{16p^2}{27} < p^2$. Thus, $(a_1b_2 + a_2b_1)^2 < p^2$, and $a_1b_2 + a_2b_1 < p$. □

Theorem 3.6. *Define m and n as from the previous theorem. Then $\left(\frac{m}{p}\right)_3 = \left(\frac{n}{p}\right)_3 = 1$.*

Proof. Conjecture □

Theorem 3.7. *Any prime divisor of m or n is a cubic residue modulo p.*

Proof. Conjecture □

Corollary 3.7.1. *Any divisor of mn is a cubic residue modulo p.*

Proof. Immediate from the fact that the product of cubic residues is another cubic residue. □

Corollary 3.7.2. *$\left(\frac{2}{p}\right)_3 = 1$ if $2|m$ or $2|n$, where $4p = m^2 + 27n^2$. Note that $m \equiv n \pmod 2$, so restricting one of m, n to be even suffices. An equivalent statement is that if $p = M^2 + 27N^2$ for integers M, N, then $\left(\frac{2}{p}\right)_3 = 1$.*

Proof. A direct result of the theorem.

A couple trivially easy to see examples are: $p = 31, 43, 127, 157, 223, 229, 277, 283, 307, 397, 433, 439, 457, 499, 601, 643, 691, 727, 733, 739, 811, 919, 997$. We can check by hand with the following trivial simple values:

$$\begin{array}{cc}
2 \equiv 4^3 \pmod{31} & 2 \equiv 14^3 \pmod{457} \\
2 \equiv 20^3 \pmod{43} & 2 \equiv 10^3 \pmod{499} \\
2 \equiv 32^3 \pmod{127} & 2 \equiv 54^3 \pmod{601} \\
2 \equiv 62^3 \pmod{157} & 2 \equiv 61^3 \pmod{643} \\
2 \equiv 68^3 \pmod{223} & 2 \equiv 94^3 \pmod{691} \\
2 \equiv 52^3 \pmod{229} & 2 \equiv 9^3 \pmod{727} \\
2 \equiv 152^3 \pmod{277} & 2 \equiv 339^3 \pmod{733} \\
2 \equiv 120^3 \pmod{283} & 2 \equiv 29^3 \pmod{739} \\
2 \equiv 52^3 \pmod{307} & 2 \equiv 23^3 \pmod{811} \\
2 \equiv 53^3 \pmod{397} & 2 \equiv 25^3 \pmod{919} \\
2 \equiv 72^3 \pmod{433} & 2 \equiv 114^3 \pmod{997}. \\
2 \equiv 13^3 \pmod{439} &
\end{array}$$

□

Corollary 3.7.3. *It is always possible to write a prime $p \equiv 1 \pmod 3$ as $p = A^2 + AB + B^2$ where $A, B, \in \mathbb{Z}^+$. If $3|B$, then $\left(\frac{C}{p}\right)_3 = 1$ where C is a divisor of $\frac{B}{3}$.*

Proof. Let $B = 3b$. Then $p = A^2 + 3Ab + 9b^2$, so $4p = 4A^2 + 12Ab + 36b^2 = (2A + 3b)^2 + 27b^2$. A direct application of the theorem finishes the proof.

For some numerical examples: $p = 439 = 5^2 + 5 \cdot 18 + 18^2$. Then $4p = 1756 = 28^2 + 27 \cdot 6^2$. We see that

$$\begin{aligned}
6 &\equiv 384^3 \pmod{439} \\
3 &\equiv 401^3 \pmod{439} \\
2 &\equiv 13^3 \pmod{439}.
\end{aligned}$$

Another example is $p = 601 = 1^2 + 1 \cdot 24 + 24^2$. Then $4p = 2404 = 26^2 + 27 \cdot 8^2$. We see that

$$\begin{aligned}
2 &\equiv 54^3 \pmod{601} \\
4 &\equiv 512^3 \pmod{601} \\
8 &\equiv 2^3 \pmod{601}.
\end{aligned}$$

A final example is $p = 1597 = 7^2 + 7 \cdot 36 + 36^2$. Then $4p = 6388 = 50^2 + 27 \cdot 12^2$.

We see that

$$\begin{aligned} 2 &\equiv 647^3 \pmod{1597} \\ 3 &\equiv 517^3 \pmod{1597} \\ 4 &\equiv 171^3 \pmod{1597} \\ 6 &\equiv 726^3 \pmod{1597} \\ 12 &\equiv 204^3 \pmod{1597}. \end{aligned}$$

□

Theorem 3.8. 2 *is a cubic residue modulo* p *if and only if* p *can be represented as* $M^2 + 27N^2$ *for integers* M, N.

Proof. Conjecture □