

1 Sample Problems

1. Show that $\mathbb{Z}[\sqrt{-26}]$ does not have unique factorization by factoring 27 in two different ways. Make sure you prove your factors are "prime."

27 can be factored normally as $3 \cdot 3 \cdot 3 = 3^3$. It can also be factored as $27 = (1 + \sqrt{-26})(1 - \sqrt{-26})$. Notice that they have a different number of factors, so they cannot be the same factorization.

To prove that 3 and $1 + \sqrt{-26}$ are prime, we may use the norm function on $\mathbb{Q}(\sqrt{-26})$, which is $N(a + b\sqrt{-26}) = a^2 + 26b^2$. Note that $N(\alpha\beta) = N(\alpha)N(\beta)$ (this is apparent using $N(\alpha) = \alpha\alpha'$). So suppose $3 = \alpha\beta$ and $1 + \sqrt{-26} = \gamma\delta$. Then $9 = N(3) = N(\alpha)N(\beta)$ and $27 = N(1 + \sqrt{-26}) = N(\gamma)N(\delta)$. If any one of these norms is 1, then the algebraic integer is 1 or -1. Otherwise, at least one of them must be 3. But $a^2 + 26b^2 = 3$ has no solutions over the integers, so no such algebraic integer exists. Hence, any factorization of 3 or $1 + \sqrt{-26}$ has a ± 1 in it, which proves they are primes in $\mathbb{Z}[\sqrt{-26}]$.

2. Let n be a positive integer greater than 1, and let a be an integer relatively prime to n . Show that $\{ka \mid 1 \leq k \leq n-1, \gcd(k, n) = 1\}$ are all distinct modulo n .

Suppose not. Then there are two integers $k \neq l$ between 1 and $n-1$ such that $ka \equiv la \pmod{n}$. Then $ka - la \equiv (k-l)a \equiv 0 \pmod{n}$. Since a is relatively prime to n , it has an inverse a^{-1} modulo n . Multiplying it on both sides results in $k - l \equiv a^{-1}\alpha(k-l) \equiv a^{-1} \cdot 0 \equiv 0 \pmod{n}$. This contradicts that fact that k and l are distinct between 1 and $n-1$. Hence, all the integers in the set are distinct modulo n .

Note that we did not use the condition that $\gcd(k, n) = 1$. It turns out to not be necessary in this problem. However, in the modified proof of Fermat's Little Theorem, we needed that fact that if a and k are relatively prime to n , then so is ak . Taking the product over all elements in the above set resulted in the theorem

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

when $n > 1$ and a is relatively prime to n .

3. Suppose p is an odd prime and a, b , and n are positive integers with $n > 1$ squarefree. Show that if $p = a^2 + nb^2$, then a and b are unique. Show that a and b are not unique for $4p = a^2 + 3b^2$. (Hint: Try $p = 7$.)

The first part was done in class when $n \geq 5$. Don't worry about the cases when $n = 2$ or $n = 3$. The second part was also done in class; 28 can be expressed in three different ways: $28 = (1)^2 + 3(3)^2 = (4)^2 + 3(2)^2 = (5)^2 + 3(1)^2$.

4. Compute the order of $\phi = \frac{1+\sqrt{5}}{2}$ modulo 7 and modulo 11. (Hint: Use Fermat's Little Theorem and $\phi' = -\frac{1}{\phi}$.)

Fermat's Little Theorem for algebraic integers states that

$$\phi^p \equiv \begin{cases} \phi \pmod{p} & \text{if } \left(\frac{5}{p}\right) = 1 \\ \phi' \pmod{p} & \text{if } \left(\frac{5}{p}\right) = -1 \end{cases}$$

Let $p = 7$. Since $\left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1$, $\phi^7 \equiv \phi' \pmod{7}$. Multiplying both sides by ϕ gives $\phi^8 \equiv \phi \cdot \phi' = -1 \pmod{7}$. Squaring both sides results in $\phi^{16} \equiv 1 \pmod{7}$. Hence, the order of ϕ divides 16. But since $\phi^8 \not\equiv 1 \pmod{7}$, this shows that no proper divisor of 16 works. Hence the order of ϕ is **16** modulo 7.

Let $p = 11$. Since $\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1$, $\phi^{11} \equiv \phi \pmod{11}$. Multiplying both sides by ϕ' gives $-\phi^{10} \equiv \phi^{10} \cdot \phi \cdot \phi' \equiv \phi \cdot \phi' = 1 \pmod{11}$. Hence, $\phi^{10} \equiv 1 \pmod{11}$, and so the order divides 10. We must now show that ϕ , ϕ^2 , and ϕ^5 is not congruent to 1 modulo 11. $\phi \not\equiv 1 \pmod{11}$, $\phi^2 = \phi + 1 \not\equiv 1 \pmod{11}$, and $\phi^5 = (\phi^2)^2 \cdot \phi = (\phi + 1)^2 \cdot \phi = (\phi^2 + 2\phi + 1) \cdot \phi = (3\phi + 2) \cdot \phi = 3\phi^2 + 2\phi = 3(\phi + 1) + 2\phi = 5\phi + 3 \not\equiv 1 \pmod{11}$. Therefore, the order of ϕ is **10** modulo 11.

5. Use the Lucas-Lehmer test to show that $2^{11} - 1$ is not prime and $2^{13} - 1$ is a prime. (It's okay to use a calculator on this one.)

We only need to calculate S_n modulo $2^{11} - 1 = 2047$ and $2^{13} - 1 = 8191$ up to $n = p - 1$ and check whether $S_{10} \equiv 0 \pmod{2047}$ and $S_{12} \equiv 0 \pmod{8191}$.

Modulo 2047: $S_1 \equiv 4$, $S_2 \equiv 14$, $S_3 \equiv 194$, $S_4 \equiv 788$, $S_5 \equiv 701$, $S_6 \equiv 119$, $S_7 \equiv 1877$, $S_8 \equiv 240$, $S_9 \equiv 282$, $S_{10} \equiv 1736$. Since $S_{10} \not\equiv 0 \pmod{2047}$, 2047 is not a prime.

Modulo 8191: $S_1 \equiv 4$, $S_2 \equiv 14$, $S_3 \equiv 194$, $S_4 \equiv 4870$, $S_5 \equiv 3953$, $S_6 \equiv 5970$, $S_7 \equiv 1857$, $S_8 \equiv 36$, $S_9 \equiv 1294$, $S_{10} \equiv 3470$, $S_{11} \equiv 128$, $S_{12} \equiv 0$. Since $S_{12} \equiv 0 \pmod{8191}$, 8191 is a prime.