Math 346/Math 377 Number Theory, Winter 2015
Homework 1 Solutions

Problems marked with an asterisk (*) are compulsory for only the students who are registered in Math 377.

(1) (a) Suppose that \( b \neq s \) but \( a + b\sqrt{2} = r + s\sqrt{2} \). Then rearranging the equation gives \( \frac{r-s}{a+b} = \sqrt{2} \), which would imply that \( \sqrt{2} \) is rational. Thus, \( b = s \), which then implies that \( a = r \).

(b) It suffices to show that every \( a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}] \) has its inverse in \( \mathbb{Q}[\sqrt{2}] \) as well. If \( b \neq 0 \), this expression rearranges to \( \frac{a-s}{b} = 2 \), which implies that \( \sqrt{2} \) is irrational. This is absurd, so we must have \( b = 0 \). This implies that \( a = 0 \) as well, and hence \( x = 0 \).

(b) \( N(xy) = (xy)(\bar{xy}) = (x\bar{x})(y\bar{y}) = N(x)N(y) \) (or you could check it directly by setting \( x = a + b\sqrt{2} \) and \( y = c + d\sqrt{2} \)).

(3) (a) By definition, it suffices to show that \( \frac{1}{17+12\sqrt{2}} \in \mathbb{Z}[\sqrt{2}] \). We have \( \frac{1}{17+12\sqrt{2}} = \frac{17-12\sqrt{2}}{17^2-2(12)^2} = 17 - 12\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \), as required.

(b) We first note that if \( x \in \mathbb{Z}[\sqrt{2}] \), then \( x \) can be written as \( a + b\sqrt{2} \), where \( a, b \in \mathbb{Z} \). Thus, \( N(x) \in \mathbb{Z} \) if \( x \in \mathbb{Z}[\sqrt{2}] \) (side note: but note that the converse is not true; one can find an element in \( \mathbb{Q}[\sqrt{2}] - \mathbb{Z}[\sqrt{2}] \) whose norm is an integer!). If \( x \) is a unit, then by definition, \( x, \frac{1}{x} \in \mathbb{Z}[\sqrt{2}] \), and so \( N(x), N(1/x) \in \mathbb{Z} \). But also, by question 2(a), we know that \( N(x)N(1/x) = 1 \). The only two integers that multiply to 1 are \( \pm 1 \), so \( N(x) = \pm 1 \).

Conversely, if \( N(x) = \pm 1 \), then \( \frac{1}{x} = \frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-2b^2} \) is a unit, then by definition, \( \sqrt{2} \) is irrational. This implies that \( a + b\sqrt{2} \) is a unit, so \( \frac{1}{x} \in \mathbb{Z}[\sqrt{2}] \).

(4) (a) We notice that \( 2 = (\sqrt{2})^2 = 2 \), \( \sqrt{2} \) is not a unit. Similarly, we notice that \( 7 = (3 + \sqrt{2})(3 - \sqrt{2}) \), and \( N(3 + \sqrt{2}) = N(3 - \sqrt{2}) = 7 \), so both factors are not units. Thus, \( 2 \) and \( 7 \) are not primes.

(b) Suppose that \( 5 - 2\sqrt{2} = ab \), with \( a, b \in \mathbb{Z}[\sqrt{2}] \). Then \( N(ab) = N(5 - 2\sqrt{2}) = 17 \), but \( N(ab) = N(a)N(b) \) by question 2(b) as well. Since \( N(a) \) and \( N(b) \) must be integers, one of \( N(a) \) or \( N(b) \) must be 1 (and the other 17), which implies that \( a \) or \( b \) is a unit, by question 3(b).

(c) \( N(3) = 9 \), so if \( 3 \) were not a prime, there exist \( a, b \in \mathbb{Z}[\sqrt{2}] \) such that \( N(a) = N(b) = \pm 3 \). We will show that no element in \( \mathbb{Z}[\sqrt{2}] \) has norm \( \pm 3 \). That is, the equation \( r^2 - 2s^2 = 3 \) has no solutions. Write \( r = 8s + t, s = 8u + v \), where \( 0 \leq t, v < 8 \). Then \( r^2 - 2s^2 = 64s^2 + 16st + t^2 - 128u^2 - 32uv - 2v^2 \). In particular, the remainder of \( r^2 - 2s^2 \), when divided by 8, is equal to the remainder of \( t^2 - 2v^2 \) when divided by 8, with \( 0 \leq t, v < 8 \). One can check that this remainder is never \( \pm 3 \).
(5) (a) Although all four terms are indeed primes, we should consider these two factorizations to be the same, because they differ "up to units", much like having unique factorization "up to signs" in the integers. For example, we check that \(\sqrt{2} - 1\) is a unit by computing the norm, and that \((3\sqrt{2} + 1)(\sqrt{2} - 1) = 5 - 2\sqrt{2}\), and similarly, \((3\sqrt{2} - 1)(\sqrt{2} + 1) = 5 + 2\sqrt{2}\). Thus, these two factorizations are related.

(b) (*) By question 3(a), if we set \(n_1 = 17, m_1 = 12\), then \(n_1^2 - 2m_1^2 = N(17 + 12\sqrt{2}) = 1\), so this is one solution to the equation \(n^2 - 2m^2 = 1\). Now, if \(17 + 12\sqrt{2}\) is a unit, then so is \((17 + 12\sqrt{2})^s\) for any \(s \in \mathbb{Z}\), by question 3(b). That is, if we write \((17 + 12\sqrt{2})^s = n_s + m_s\sqrt{2}\), then \((n_s, m_s)\) is a solution to the equation \(n^2 - 2m^2 = 1\). Furthermore, we note that \(n_{s-1} < n_s\), so these solutions are all distinct. Thus, there are infinitely many integer solutions of \(n^2 - 2m^2 = 1\).

(6) We will show that (1) \(\Rightarrow\) (2) \(\Rightarrow\) (3) \(\Rightarrow\) (1).

(1) \(\Rightarrow\) (2): If \(\alpha\) satisfies \(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0\) with \(a_i \in \mathbb{Z}\), then we claim that \(\mathbb{Z}[\alpha]\) can be generated by 1, \(\alpha, \ldots, \alpha^{n-1}\). Indeed, \(\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0\), with \(a_i \in \mathbb{Z}\), and we can recursively obtain expressions of \(\alpha^k\) for \(k \geq n\) using the above expression.

(2) \(\Rightarrow\) (3): Set \(R = \mathbb{Z}[\alpha]\).

(3) \(\Rightarrow\) (1): Suppose that \(\{e_1, \ldots, e_n\}\) is the generator of \(R\) with \(\mathbb{Z}\)-coefficients. Then multiplication by \(\alpha\) in \(R\) can be represented by an \(n \times n\) matrix with integral entries. It follows that the characteristic polynomial of this matrix is monic and has \(\alpha\) as a solution, by the Cayley-Hamilton theorem.

(7) Suppose that \(1, \alpha, \ldots, \alpha^n\) generates \(\mathbb{Z}[\alpha]\), and \(1, \beta, \ldots, \beta^m\) generates \(\mathbb{Z}[\beta]\), both over \(\mathbb{Z}\) (such generators must exist by problem 6). Then we can show that \(\mathbb{Z}[\alpha, \beta]\) is generated by the finite set \(\{\alpha^i\beta^j \mid 1 \leq i \leq n, 1 \leq j \leq m\}\) over \(\mathbb{Z}\). Since \(\alpha + \beta, \alpha\beta \in \mathbb{Z}[\alpha, \beta]\), it follows by problem 6, third criterion that \(\alpha + \beta\) and \(\alpha\beta\) are algebraic integers.

(8) I claim that the string of 2015 numbers \((2016)!+2, (2016)!+3, (2016)!+4, \ldots, (2016)!+2016\) are all composite. Indeed, for \(2 \leq j \leq 2016, j|(2016)! + j\), so every number in the sequence is composite. (Note that \(n!\) means \(1 \cdot 2 \cdots n\).

(9) Suppose that there are only finitely many primes of the form \(4n + 3\). We list them as \(3 = p_1 < p_2 < \cdots < p_k\). Now, consider \(m = 4p_2 \cdots p_k + 3\). We note that \(3 \nmid m\), and also \(p_j \nmid m\) for \(2 \leq j \leq k\). Thus, if a prime factorization of \(m\) existed, all of its prime factors must be of the form \(4n + 1\). However, multiplying all of these factors together yields another integer of the form \(4\ell + 1\). This contradicts the construction of the \(m\), i.e. it is of the form \(4N + 3\). Since \(m\) is larger than any of the \(p_i\) with \(1 \leq i \leq k\), we have found a number that is not in the list of primes of the forms of \(4n + 3\), yet does not admit a prime factorization with the list of known primes. This implies that there are infinitely may primes of the form \(4n + 3\).