MEMORIAL UNIVERSITY OF NEWFOUNDLAND

DEPARTMENT OF MATHEMATICS AND STATISTICS

FALL 2005 **PMAT 3370** WORKSHEET SOLUTIONS

Marks

[4] 1. Compute a gcd of $\alpha = 26 + 7i$ and $\beta = -59 - 17i$, by copying the method for rational integers. Write the gcd in the form $\alpha\lambda + \beta\sigma$.

Solution: We have $\frac{\beta}{\alpha} = \frac{-59-17i}{26+7i} = \frac{-1653}{725} - \frac{29}{725}i = -\frac{57}{25} - \frac{1}{25}i$. Hence, $q_1 = -2 + 0i$ and $\beta = \alpha(-2) + (-7 - 3i)$. Similarly, $\frac{26+7i}{-7-3i} = \frac{-203}{58} + \frac{29}{58}i = -\frac{7}{2} + \frac{1}{2}i$. Hence, choose $q_2 = -3$ (or $-3 + i$ or -4 or $-4 + i$) and then $26 + 7i = (-7 - 3i)(-3) + (5 - 2i)$. Since $\frac{-7-3i}{5-2i} = \frac{-29-29i}{29} = -1 - i \in G$, then $-7 - 3i = (5 - 2i)(-1 - i) + 0$. Hence a gcd of α and β is $5 - 2i$ the last nonzero remainder. (The other possible gcd's are the associates $-5 + 2i, 2 + 5i, -2 - 5i$.) We have $5 - 2i = 26 + 7i - [(-59 - 17i) - (26 + 7i)(-2)](-3)$. Hence

$$5 - 2i = (-59 - 17i)3 + (26 + 7i)7.$$

[3] 2. Let α and β be Gaussian integers. If $\alpha \mid \beta$, prove that $N(\alpha) \mid N(\beta)$. Is the converse true?

Solution: Since $\alpha \mid \beta$, then $\beta = \alpha\gamma$ where $\gamma \in G$. Then $N(\beta) = N(\alpha\gamma) = N(\alpha)N(\gamma)$. Since $N(\alpha), N(\beta), N(\gamma)$ are rational integers, then clearly $N(\alpha) \mid N(\beta)$.

The converse is not true. For example, $N(2 + 3i) \mid N(2 - 3i)$ but $(2 + 3i) \not\mid (2 - 3i)$.

[7] 3. (a) Find a gcd of $\alpha = -172 + 210i$ and $\beta = 624 - 52i$.

Solution: We use the Division Algorithm until we get a zero remainder:

$$\begin{aligned}
\beta &= \alpha(-2 - 2i) + (-140 + 24i) \\
\alpha &= (-140 + 24i)(1 - i) + (-56 + 46i) \\
-140 + 24i &= (-56 + 46i)(2 + i) + (18 - 12i) \\
-56 + 46i &= (18 - 12i)(-3) + (-2 + 10i) \\
18 - 12i &= (-2 + 10i)(-1 - i) + (6 - 4i) \\
-2 + 10i &= (6 - 4i)(-1 + i) + 0.
\end{aligned}$$

Hence a gcd is $6 - 4i$, the last nonzero remainder.

(b) Factor α and β completely into primes and hence check your answer in part (a).
Solution: With help from Maple we have

$$\begin{aligned}\alpha &= (-1)(1+i)^2(3-2i)^2(3-10i)\\ \beta &= i(1+i)^4(3+2i)(3-2i)(-1-2i)(-5-2i).\end{aligned}$$

Therefore a gcd is $(1+i)^2(3-2i) = 2i(3-2i) = i(6-4i)$.

[3] 4. Let $\mathbb{Z}[\sqrt{-2}] = \{a+b\sqrt{-2} \mid a,b \in \mathbb{Z}\}$. Then the norm map N is defined in exactly the same way in this set of "integers", namely, for $\alpha = a+b\sqrt{-2}$, $N(\alpha) = \alpha\overline{\alpha} = a^2+2b^2$. State and prove a Division Algorithm for $\mathbb{Z}[\sqrt{-2}]$.

Solution: If $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$ and $\alpha \neq 0$, then there exist $q, r \in \mathbb{Z}[\sqrt{-2}]$ such that $\beta = \alpha q + r$ where $N(r) < N(\alpha)$.

Proof: Consider $\dfrac{\beta}{\alpha} = \dfrac{\beta\bar{\alpha}}{\alpha\bar{\alpha}} = A + B\sqrt{-2}$ where $A, B \in \mathbb{Q}$. (Note $\dfrac{\beta}{\alpha} = \dfrac{a+b\sqrt{-2}}{c+d\sqrt{-2}} = \dfrac{(a+b\sqrt{-2})(c-d\sqrt{-2})}{c^2+2d^2} = \dfrac{ac+2bd}{c^2+2d^2} + \dfrac{bc-ad}{c^2+2d^2}\sqrt{-2}$.) Choose $a, b \in \mathbb{Z}$ such that $|A-a| \leq \frac{1}{2}$ and $|B-b| \leq \frac{1}{2}$. Let $q = a+b\sqrt{-2}$, and $r = \beta - \alpha q$. Then clearly $\beta = \alpha q + r$ and

$$\begin{aligned}N(r) &= N(\beta-\alpha q) = N(\alpha)N(\frac{\beta}{\alpha} - q) = N(\alpha)N((A-a)+(B-b)\sqrt{-2})\\ &= N(\alpha)((A-a)^2+2(B-b)^2) \leq N(\alpha)(\frac{1}{4}+\frac{2}{4}) = \frac{3}{4}N(\alpha) < N(\alpha).\end{aligned}$$

[8] 5. Prove that you cannot have a Division Algorithm in the "rings" $\mathbb{Z}[\sqrt{-5}]$, $\mathbb{Z}[\sqrt{-6}]$ and $\mathbb{Z}[\sqrt{-10}]$ by examining the factorizations $3\cdot 7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$, $2\cdot 3 = -\sqrt{-6}\sqrt{-6}$ and $2\cdot 5 = -\sqrt{-10}\sqrt{-10}$. (You should first show that the set of units in these three rings is $\{\pm 1\}$).

Solution: It is straightforward to prove that ϵ is a unit if and only if $N(\epsilon) = 1$ for $\epsilon \in \mathbb{Z}[\sqrt{-d}]$ where d is positive and square-free. Hence ϵ is a unit if and only if $a^2+db^2 = 1$ for some $a, b \in \mathbb{Z}$. But if $d > 1$, then the only solutions are $b = 0, a = \pm 1$. Hence the set of units is $\{\pm 1\}$.

In the set $\mathbb{Z}[\sqrt{-5}]$, we first prove that 3, 7, $1+2\sqrt{-5}$ and $1-2\sqrt{-5}$ are primes. If 3 is NOT a prime, then $3 = \alpha\beta$ for $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$. Then $9 = N(\alpha)N(\beta)$ and so $N(\alpha) = 3 = N(\beta)$ if neither α nor β is a unit. Let $\alpha = a+b\sqrt{-5}$, then $3 = N(\alpha) = a^2+5b^2$. Clearly this (Diophantine) equation has no solutions. Hence 3 is prime. In exactly the same

way, one shows that 7, $1 \pm 2\sqrt{-5}$ are primes. Hence 21 has two different factorizations into primes. Hence there is no unique factorization into primes in $\mathbb{Z}[\sqrt{-5}]$, and hence no Division Algorithm.

In $\mathbb{Z}[\sqrt{-6}]$ the only units are ± 1. We need to prove that 2, 3, $\pm\sqrt{-6}$ are primes in $\mathbb{Z}[\sqrt{-6}]$. If 2, say, in NOT prime then $2 = \alpha\beta$ and $4 = N(\alpha)N(\beta)$ so $N(\alpha) = 2 = N(\beta)$ since α and β are not units. Let $\alpha = a + b\sqrt{-6}$, then $2 = a^2 + 6b^2$. Clearly there are no solution to this (Diophantine) equation. Similarly for 3 and $\pm\sqrt{-6}$. Say $-\sqrt{-6} = \alpha\beta$, then $6 = N(-\sqrt{-6}) = N(\alpha)N(\beta)$ and hence $N(\alpha) = 2$ or 3. If $\alpha = a + b\sqrt{-6}$, then $a^2 + 6b^2 = 2$ or 3 clearly have no solutions. As in the case above, the factorizations $2(3) = -\sqrt{-6}\sqrt{-6}$ show that there is no unique factorization into primes, and hence no Division Algorithm.

Similarly in $\mathbb{Z}[\sqrt{-10}]$, $a^2 + 10b^2 = 2$ or 5 have no solutions etc.

The norm map N can be defined in the setting $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ where d is a square free positive integer greater than 1. For $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, $N(\alpha) = \alpha\overline{\alpha} = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$. Prove that $N(\alpha\beta) = N(\alpha)N(\beta)$ for $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$.

Solution: Let $\alpha = a + b\sqrt{d}$ and $\beta = c + e\sqrt{d}$. Then $\alpha\beta = ac + bed + (ae + bc)\sqrt{d}$ so $N(\alpha\beta) = (ac + bed)^2 - d(ae + bc)^2 = a^2c^2 + 2abcde + b^2e^2d^2 - da^2e^2 - 2abcde - db^2c^2 = a^2c^2 + b^2e^2d^2 - da^2e^2 - db^2c^2 = (a^2 - db^2)(c^2 - de^2) = N(\alpha)N(\beta)$.

Show that $\mathbb{Z}[\sqrt{10}]$ does not have a Division Algorithm by examining the factorization $2 \cdot 5 = (\sqrt{10})^2$.

Solution: First, we show that ϵ is a unit in $\mathbb{Z}[\sqrt{d}]$ if and only if $N(\epsilon) = \pm 1$.

Proof: If ϵ is a unit then $\epsilon\epsilon' = 1$ for some $\epsilon' \in \mathbb{Z}[\sqrt{d}]$. Computing the norm we have $N(1) = N(\epsilon)N(\epsilon')$. Since $N(1) = 1$ and $N(\epsilon)$ and $N(\epsilon')$ are rational integers, then $N(\epsilon) = \pm 1$. Conversely, if $\pm 1 = N(\epsilon) = \epsilon\bar{\epsilon}$, then clearly $\epsilon \mid 1$ so ϵ is a unit.

Suppose 2 is not a prime in $\mathbb{Z}[\sqrt{10}]$. Then $2 = \alpha\beta$ for $\alpha, \beta \in \mathbb{Z}[\sqrt{10}]$, where neither α nor β is a unit. Since $4 = N(\alpha)N(\beta)$, then $N(\alpha) = \pm 2$. Let $\alpha = a + b\sqrt{10}$, then $a^2 + 10b^2 = \pm 2$. Hence $a^2 \equiv \pm 2 \pmod 5$. This is clearly impossible, since the squares modulo 5 are 0, 1 and 4. In a similar way one can show that 5 and $\sqrt{10}$ are primes in $\mathbb{Z}[\sqrt{10}]$. (It is clear that no two of these primes are associates. Why?)

---

[25]