M E T U
Mathematics Department

Math 366	Elementary Number Theory II	Spring 2017	MIDTERM 2

Küçüksakallı **April 27, 2017** **17:40 – 19:40**	Name : Last Name :	Student Number : Signature :

P.1 / 25	P.2 / 25	P.3 / 25	P.4 / 25	**SHOW YOUR ORGANIZED WORK**	**Total** / **100**
				GOOD LUCK!	

Q.1) a) Show that $\sqrt{11} = [3; \overline{3, 6}\,]$.

We have $3 < \sqrt{11} < 4$. Thus $a_0 = 3$. We observe that

$$3 < \frac{1}{\sqrt{11}-3} = \frac{\sqrt{11}+3}{2} < 4.$$

It follows that $a_1 = 3$. Next, we find that

$$6 < \frac{1}{\frac{\sqrt{11}+3}{2} - 3} = \frac{2}{\sqrt{11}-3} = \sqrt{11}+3 < 7,$$

and $a_2 = 6$. Finally, we see that

$$3 < \frac{1}{\sqrt{11}+3-6} = \frac{\sqrt{11}+3}{2} < 4,$$

and therefore $a_3 = 3$. From this point on, the pattern is obvious.

b) Let (x_n, y_n) be a solution of $x^2 - 11y^2 = 1$. For each nonnegative integer n, show that $(x_{n+1}, y_{n+1}) = (10x_n + 33y_n, 3x_n + 10y_n)$ is a solution of $x^2 - 11y^2 = 1$.

This can be verified by direct substitution. More precisely,

$$\begin{aligned}
x_{n+1}^2 - 11y_{n+1}^2 &= (10x_n + 33y_n)^2 - 11(3x_n + 10y_n)^2 \\
&= (100x_n^2 + 660x_ny_n + 1089y_n^2) - 11(9x_n^2 + 60x_ny_n + 100y_n^2)^2 \\
&= x_n^2 - 11y_n^2 = 1.
\end{aligned}$$

c) Is there a solution of $x^2 - 11y^2 = 1$ with $1000 < x < 2000$?

The fundamental solution of $x^2 - 11y^2 = 1$ is $(x_1, y_1) = (10, 3)$. This can be obtained by the first convergent of $[3; \overline{3, 6}\,]$, or by trying $y = 1, 2$ and 3. All positive solutions are of the form (x_n, y_n) where $x_n + y_n\sqrt{11} := (x_1 + y_1\sqrt{11})^n$. We compute that $(x_2, y_2) = (199, 60)$ and $(x_3, y_3) = (3970, 1197)$. We know that $x_k > x_3 > 2000$ for all $k > 3$. Thus we conclude that there is no solution with $1000 < x < 2000$.

Q.2) Show that an integer n can be represented as the difference of two squares if and only if n is not of the form $4k+2$.

($\Leftarrow$) Any odd integer $n = 2m+1$ can be expressed as the difference of two squares since $(m+1)^2 - m^2 = 2m+1$. It remains to consider the integers $n \equiv 0 \pmod 4$. In such a case, we have $n = 4\ell$ for some integer ℓ and $n = (\ell+1)^2 - (\ell-1)^2$.

($\Rightarrow$) A square is either 0 or 1 modulo 4. If $n = x^2 - y^2$, we see that $n \not\equiv 2 \pmod 4$.

Q.3) Show that there are infinitely many primitive Pythagorean triples $x^2 + y^2 = z^2$ with $y - x = 7$. For example $(5, 12, 13), (8, 15, 17), (48, 55, 73), \dots$ etc.

It is enough to find infinitely many a and b such that $a^2 - b^2 - 2ab = 7$. Using the transformation $u = a - b$ and $v = b$, this equation becomes $u^2 - 2v^2 = 7$. Since $a = u + v$ and $b = v$, it is enough to show that $u^2 - 2v^2 = 7$ has infinitely many positive solutions (i.e. $u > 0, v > 0$).

It is easy to see that $(u_0, v_0) = (3, 1)$ is a solution of $u^2 - 2v^2 = 7$. Define $\alpha = 3 + \sqrt{2}$ with $N(\alpha) = 7$ and $\varepsilon = 3 + 2\sqrt{2}$ with $N(\varepsilon) = 1$. Observe that $N(\alpha \cdot \varepsilon^n) = N(\alpha)N(\varepsilon)^n = 7 \cdot 1^n = 7$ for all $n \in \mathbb{N}$. We define (u_n, v_n) as follows

$$u_n + v_n\sqrt{2} = \alpha \cdot \varepsilon^n.$$

Observe that

$$u_n^2 - 2v_n^2 = N(u_n + v_n\sqrt{2}) = N(\alpha \cdot \varepsilon^n) = 7.$$

Moreover $v_{n+1} = 2u_n + 3v_n > v_n$ for each $n \in \mathbb{N}$. The equation $u^2 - 2v^2 = 7$ has infinitely many positive solutions.

Q.4) Consider the Gaussian integers $\alpha = 7 - i$ and $\beta = 3 + 4i$.

a) Represent α and β as a product of Gaussian primes. Show that $\beta \nmid \alpha$ in $\mathbb{Z}[i]$.

We have $\alpha = (1+i)(2-i)^2$ and $\beta = (2+i)^2$. The Gaussian integer α has no prime factor divisible by $2+i$, whereas β has. Since $\mathbb{Z}[i]$ is a UFD, we conclude that $\beta \nmid \alpha$.

b) Show that $\gcd(\alpha, \beta) = 1$ by using the Euclidean algorithm.

We apply the Euclidean algorithm and find that

$$\begin{aligned} \alpha &= \beta(1-i) - 2i \\ \beta &= (-2i)(-2+2i) - 1 \\ -2i &= (-1)(2i) + 0 \end{aligned}$$

We conlude that $\gcd(\alpha, \beta) = -1$. Recall that $\gcd(\alpha, \beta)$ in $\mathbb{Z}[i]$ is well defined up to a unit.

c) Find Gaussian integers η and λ such that $\alpha\eta + \beta\lambda = 1$.

Applying the Euclidean algorithm in reverse, we find that

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

We may choose $\eta = -2 + 2i$ and $\lambda = -1 - 4i$.

d) Find Gaussian integers η and λ such that $\alpha\eta + \beta\lambda = 1$ and $\eta \in \mathbb{Z}$.

Observe that $(\eta, \lambda) = (-2 + 2i + x\beta, -1 - 4i - x\alpha)$ satisfies the condition $\alpha\eta + \beta\lambda = 1$ for each $x \in \mathbb{Z}[i]$. If $x = a + bi$, then the imaginary part of η is $4a + 3b + 2$. Choosing $a = 1$ and $b = -2$, we find that $(\eta, \lambda) = (9, -6 + 11i)$ satisfies the desired conditions.

Q.5) Prove or disprove: *All integers can be expressed as a sum of two Gaussian integer squares.* (For example $7 = (4 + 0 \cdot i)^2 + (0 + 3 \cdot i)^2$.)

We know, by **(Q.2)**, that any integer which is not of the form $4k + 2$ can be expressed as the difference of two squares. Such an integer can also be expressed as a sum of two Gaussian integer squares. More precisely, it can be expressed in the form $(x + 0 \cdot i)^2 + (0 + y \cdot i)^2 = x^2 - y^2$. It remains to consider integers n which are of the form $4k + 2$. Note that

$$\begin{aligned} 4k + 2 &= 2(2k + 1) \\ &= 2((k + 1)^2 - k^2) \\ &= \left[(k + 1)^2 + 2k(k + 1)i - k^2\right] + \left[(k + 1)^2 - 2k(k + 1) - k^2\right] \\ &= (k + 1 + ki)^2 + (k + 1 - ki)^2. \end{aligned}$$

Therefore any integer can be expressed as a sum of two Gaussian integer squares.

Q.6) Recall that we have mentioned in class that $r_2(n)/4$ is a multiplicative function but we didn't prove it. This question concerns a special case. If p and q are distinct primes, then show that $r_2(pq)/4 = [r_2(p)/4] \cdot [r_2(q)/4]$.

It is trivially true that $r_2(2) = 4$. Recall that $r_2(p) = 0$ if $p \equiv 3 \pmod 4$. Moreover, $r_2(p) = 8$ if $p \equiv 1 \pmod 4$ since the representation $p = x^2 + y^2$ is unique up to the order and signs.

Now let us consider the formula $r_2(pq)/4 = [r_2(p)/4] \cdot [r_2(q)/4]$. A positive integer $n = pq$ can be represented as a sum of two squares if and only if its square free part has no prime factor of the form $4k + 3$. If one of p or q is of the form $4k + 3$, then both sides are zero and the formula is trivially true.

If $2 \in \{p, q\}$, then without loss of generality $p = 2$ and q is of the form $4k + 1$. We have $r_2(p) = 4$ and $r_2(q) = 8$. Let $\pi \in \mathbb{Z}[i]$ be a Gaussian prime of norm q. An element $\alpha \in \mathbb{Z}[i]$ of norm pq must be of the form

$$\alpha = i^{k_1}(1 + i)\pi^{k_2}\overline{\pi}^{1-k_2}$$

where $0 \leq k_1 \leq 3$ and $0 \leq k_2 \leq 1$. There are 8 such elements. Thus $r_2(pq)/4 = 2$ and this finishes the proof for this case.

It remains to consider both p and q are of the form $4k + 1$. We have $r_2(p) = r_2(q) = 8$. Let π_1 and π_2 be two Gaussian primes of norms p and q, respectively. An element $\alpha \in \mathbb{Z}[i]$ of norm pq must be of the form

$$\alpha = i^{k_1}\pi_1^{k_2}\overline{\pi}_1^{1-k_2}\pi_2^{k_3}\overline{\pi}_2^{1-k_3}$$

where $0 \leq k_1 \leq 3$ and $0 \leq k_2, k_3 \leq 1$. There are 16 such elements. Thus $r_2(pq)/4 = 4$ and this finishes the proof