Kris Harper
MATH 24200
April 12, 2010

Homework 1

Problem 1. *Prove that $\sqrt[n]{m}$ is irrational if m is not the nth power of an integer.*

Proof. Suppose $\sqrt[n]{m} = a/b$ where $a, b \in \mathbb{Z}$ and $(a, b) = 1$. Then $mb^n = a^n$. We can uniquely prime factor a and b as $p_1^{a_1} \dots p_r^{a_r}$ and $q_1^{b_1} \dots q_s^{b_s}$. Then we can group the prime factors of a^n as n identical groups of $p_1^{a_1} \dots p_r^{a_r}$. It follows that mb^n can be written as the product of n identical groups of prime powers. But then each of these groups must contain $q_1^{b_1} \dots q_s^{b_s}$ since this is the prime factorization of b. Therefore m must have a prime factorization such that it can be evenly divided into these n groups. In other words, we must have $m = c^n$ for some integer c. ☐

Problem 2. *Suppose $a^2 + b^2 = c^2$ with $a, b, c \in \mathbb{Z}$. For example $3^2 + 4^2 = 5^2$ and $5^2 + 12^2 = 13^2$. Assume that $(a, b) = (b, c) = (c, a) = 1$. Prove that there exist integers u and v such that $c - b = 2u^2$ and $c + b = 2v^2$ and $(u, v) = 1$ (there is no loss in generality in assuming that b and c are odd and a is even). Consequently $a = 2uv$, $b = v^2 - u^2$ and $c = v^2 + u^2$. Conversely show that if u and v are given, then the three numbers a, b and c given by these formulas satisfy $a^2 + b^2 = c^2$.*

Proof. Since c and b are relatively prime and both odd we can write $(c-b)(c+b)$ as $4(p_1^{a_1} p_2^{a_2} \dots p_n^{a_n})(q_1^{b_1} q_2^{b_2} \dots q_m^{b_m})$ where $2p_1^{a_1} \dots p_n^{a_n} = c - b$, $2q_1^{b_1} \dots q_m^{b_m} = c + b$, p_i, q_i are primes and $p_i \neq q_j$ for all i and j. That is, $c - b$ and $c + b$ are relatively prime except for a factor of 2. Now write $4(a/2)^2 = (c - b)(c + b)$. Now associate each of the factors corresponding to $c - b$ with the same prime factors in $(a/2)^2$. Since $c - b$ and $c + b$ share no common factors (except for 2) we see that none of the squares get split up in this process. Thus $c - b = 2r_1^{2c_1} \dots r_{n'}^{2c_{n'}} = 2u^2$ where $u = r_1^{c_1} \dots r_{n'}^{c_{n'}}$. Likewise $c + b = 2s_1^{2d_1} \dots s_{m'}^{2d_{m'}} = 2v^2$ where $v = s_1^{d_1} \dots s_{m'}^{d_{m'}}$. Since $(c - b, c + b) = 2$ and it immediately follows that $(u, v) = 1$.

Conversely, suppose we are given such u and v. Then $a^2 = 4u^2v^2 = (c - b)(c + b) = c^2 - b^2$ so we have the desired formula. ☐

Problem 3. *If $a^n - 1$ is prime, show that $a = 2$ and that n is a prime. Assume $a > 0$ and $n > 1$*

Proof. Note that $a^n - 1 \neq 2$ since the equation $a^n = 3$ has no integer solutions by Problem 1. Then $a^n - 1 = p$ where p is necessarily odd and so $a^n = p + 1$ which shows a^n is even. Therefore $2 \mid a^n$ which means $2 \mid a$ since 2 is prime. We can then write $a^n = 2^n m^n$ for some positive integer m. But now note that

$$2^n m^n - 1 = (2m - 1)(1 + 2m + 2^2 m^2 + \cdots + 2^{n-1} m^{n-1})$$

so if $m \neq 1$ we have a factorization of p. Thus $a = 2$. A similar argument shows that n must be prime because if $n = rs$ then we have

$$2^n - 1 = 2^r 2^s - 1 = (2^r - 1)(1 + 2^r + 2^{2r} + \cdots + 2^{rs-r}).$$

In order for this to be prime we must have $r = 1$ so that n is prime. ☐

Problem 4. *Prove that $\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ is not an integer.*

Proof. Find k such that $2^k \leq n \leq 2^{k+1}$. Now find the lowest common multiple of $\{2, \dots, 2^k - 1, 2^k + 1, \dots, n\}$. This will necessarily be of the form $2^{k-1}m$ where m is an odd integer. Now multiply this by the sum in question. We have

$$2^{k-1} m \left(\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \right).$$

Every term in this product is an integer except $2^{k-1}m(1/2^k) = m/2$ since m is odd. Thus the sum in question cannot be an integer. ☐

Problem 5. *Show that 3 is divisible by $(1-\omega)^2$ in $\mathbb{Z}[\omega]$.*

Proof. We have $(1-\omega)^2 = 1-2\omega+\omega^2 = 1-2\omega+(-\omega-1) = -3\omega$. Now multiply both sides by $\omega+1$. On the left we have $(\omega+1)(1-\omega)^2$ and on the right we have $3(-\omega(\omega+1)) = 3(-\omega^2-\omega) = 3(\omega+1-\omega) = 3$. Therefore $3 = (\omega+1)(1-\omega)^2$. □

Problem 6. *For $\alpha = a+b\omega \in \mathbb{Z}[\omega]$ we defined $\lambda(\alpha) = a^2-ab+b^2$. Show that α is a unit iff $\lambda(\alpha) = 1$. Deduce that 1, -1, ω, $-\omega$, ω^2 and $-\omega^2$ are the only units in $\mathbb{Z}[\omega]$.*

Proof. Suppose $\alpha = a+b\omega$ is a unit with inverse $\beta = c+d\omega$. Note that λ is multiplicative so we have $1 = \lambda(\alpha\beta) = \lambda(\alpha)\lambda(\beta) = (a^2-ab+b^2)(c^2-cd+d^2)$. Since each of these factors is a positive integer we must have $a^2-ab+b^2 = 1$ so that $\lambda(\alpha) = 1$.

Conversely, suppose $\lambda(\alpha) = 1$. Then $a^2-ab+b^2 = 1$. We wish to find β such that $\alpha\beta = 1$. Multiplying out the terms we get the equations $ac-bd = 1$ and $ad+bc-bd = 0$. Solving the first equation for c and plugging it into the second gives us $a^2c-a+b^2c-abc+b = 0$. Using the fact that $a^2-ab+b^2 = 1$ we now have $c = a-b$. We can then use this to find $d = -b$. It's a quick check to see that $\beta = (a-b)-b\omega$ is α^{-1}. Thus α is a unit. □

Problem 7. *Define $\mathbb{Z}[\sqrt{-2}]$ as the set of all complex numbers of the form $a+b\sqrt{2}$, where $a,b \in \mathbb{Z}$. Show that $\mathbb{Z}[\sqrt{-2}]$ is a ring. Define $\lambda(\alpha) = a^2+2b^2$ for $\alpha = a+b\sqrt{2}$. Use λ to show $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain.*

Proof. Since $\mathbb{Z}[\sqrt{-2}]$ is contained in the ring $\mathbb{C}$ we need only show that $\mathbb{Z}[\sqrt{-2}]$ is nonempty and closed under subtraction and multiplication. Let $\alpha = a+b\sqrt{-2}$ and $\beta = c+d\sqrt{-2}$. Then $\alpha-\beta = (a-c)+(b-d)\sqrt{-2}$ which is in $\mathbb{Z}[\sqrt{-2}]$. Likewise $\alpha\beta = (ac-2bd)+(ad+bc)\sqrt{-2}$ which is also in $\mathbb{Z}[\sqrt{-2}]$. Thus $\mathbb{Z}[\sqrt{-2}]$ is a ring.

Let α and β be as before and suppose $\beta \neq 0$. Now $\alpha/\beta = r+s\sqrt{2}$ where $r,s \in \mathbb{Q}$. Choose integers $m,n \in \mathbb{Z}$ such that $|r-m| \leq \frac{1}{2}$ and $|s-n| \leq \frac{1}{2}$. Let $\delta = m+ni$ so that $\delta \in \mathbb{Z}[\sqrt{-2}]$. We have $\lambda(\alpha/\beta-\delta) = (r-m)^2+2(s-n)^2 \leq \frac{1}{4}+2\frac{1}{4} = \frac{3}{4}$. Let $\rho = \alpha-\beta\delta$. Then $\rho \in \mathbb{Z}[\sqrt{-2}]$ and we must have either $\rho = 0$ or

$$\lambda(\rho) = \lambda(\beta((\alpha/\beta)-\delta)) \leq \lambda(\beta)\lambda((\alpha/\beta)-\delta) \leq \frac{3}{4}\lambda(\beta) < \lambda(\beta).$$

Therefore $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain by λ. □

Problem 8. *Show that the only units in $\mathbb{Z}[\sqrt{-2}]$ are 1 and -1.*

Proof. Suppose $\alpha\beta = 1$ with $\alpha = a+b\sqrt{-2}$ and $\beta = c+d\sqrt{-2}$. Then $ac-2bd = 1$ and $ad+bc = 0$. Solving the second equation for c and plugging it into the first we see that $d = -b/(a^2+2b^2)$. Since the denominator is necessarily greater than b we see that this can only be an integer if $a^2+2b^2 = 1$. But this can only happen if $b = 0$ and $a = \pm 1$. □

Problem 9. *Suppose $\pi \in \mathbb{Z}[i]$ and that $\lambda(\pi) = p$ is a prime in $\mathbb{Z}$. Show that π is a prime in $\mathbb{Z}[i]$. Show that the corresponding result holds in $\mathbb{Z}[\omega]$ and $\mathbb{Z}[\sqrt{-2}]$.*

Proof. Suppose $\pi = \alpha\beta$. Then $p = \lambda(\pi) = \lambda(\alpha\beta) = \lambda(\alpha)\lambda(\beta)$. Since $\lambda(\alpha)$ and $\lambda(\beta)$ are both integers, we see that one of them must be 1 which means α or β is a unit in $\mathbb{Z}[i]$. Thus π must be irreducible and therefore prime since $\mathbb{Z}[i]$ is a P.I.D.. The exact same proof holds for $\mathbb{Z}[\omega]$ and $\mathbb{Z}[\sqrt{-2}]$ using Problem 6 and Problem 8 because λ is multiplicative in these cases too. □

Problem 10. *For a rational number r let $[r]$ be the largest integer less than or equal to r, e.g., $[\frac{1}{2}] = 0$, $[2] = 2$ and $[3\frac{1}{3}] = 3$. Prove $\mathrm{ord}_p n! = [n/p]+[n/p^2]+[n/p^3]+\ldots$.*

Proof. Consider the set of pairs (s,t) where $p^s t \leq n$. If we fix s we can increment t starting at $t = 1$ and stopping when $p^s t > n$. Then there's some value t_s such that $p^s t_s \leq n$ and $p^s(t_s + 1) > n$. Moreover, it's clear that $[n/p^s] = t_s$. But note that the pairs (s,t) for all integer values of $s > 0$ and $1 \leq t \leq t_s$ together represent all the possible divisors of $n!$ which include a factor of p. Therefore to count factors of p in $n!$ we need only count these pairs. But we've already seen that for each s there are t_s pairs so the total is simply $\sum_{s=1}^{\infty} t_s = \sum_{s=1}^{\infty}[n/p^s]$. $\square$

Problem 11. *Deduce from Exercise 6 that* $\text{ord}_p n! \leq n/(p-1)$ *and that* $\sqrt[n]{n!} \leq \prod p \mid n! p^{1/(p-1)}$.

Proof. We know each term in the series in Problem 10 is less than or equal to n/p^k. Thus $\text{ord}_p n! \leq \sum_{k=1}^{\infty} n/p^k = n/(p-1)$.

Since the order of each prime appearing in $n!$ is less than or equal to $n/(p-1)$ it follows that

$$n! \leq \prod_{p|n!} p^{\frac{n}{p-1}} = \left(\prod_{p|n!} p^{\frac{1}{p-1}}\right)^n$$

so $\sqrt[n]{n!} \leq \prod_{p|n!} p^{1/(p-1)}$. $\square$

Problem 12. *Use Exercise 7 to show that there are infinitely many primes.*

Proof. Suppose there are only finitely many primes $p_1, \ldots p_m$. Let $n = p_1 p_2 \ldots p_m$. Using Problem 11 and the fact that $n^n \leq (n!)^2$ we have

$$n^n \leq (n!)^2 \leq (n!)^n \leq \prod_{p|n!} p^{\frac{n}{p-1}} = \prod_{i=1}^{m} p_i^{\frac{n}{p_i - 1}} = \left(\prod_{i=1}^{m} p_i^{\frac{1}{p-1}}\right)^n < n^n$$

since $1/(p-1) \leq 1$. This is a contradiction and so there must be infinitely many primes. $\square$

Problem 13. *Consider the function* $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$. $\zeta(s)$ *is called the Riemann zeta function. It converges for* $s > 1$. *Prove the formal identity (Euler's identity)* $\zeta(s) = \prod_p (1 - (1/p^s))^{-1}$.

Proof. For each prime p multiply both sides of $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$ by $1/p^s$ and then subtract the result from the previous result. We have

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \ldots$$

and

$$\frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \ldots.$$

Subtracting we have

$$\left(1 - \frac{1}{2^s}\right)\zeta(s) = \frac{1}{1^s} + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \ldots.$$

Repeating the process for $p = 3$ we get

$$\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{2^s}\right)\zeta(s) = \frac{1}{1^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{11^s} + \ldots.$$

Applying this to every prime we arrive at the formula

$$\prod_p \left(1 - \frac{1}{p^s}\right)\zeta(s) = 1$$

which then gives the desired formula $\zeta(s) = \prod_p (1 - (1/p^s))^{-1}$. $\square$

Problem 14. *Verify the formal identities*
(a) $\zeta(s)^{-1} = \sum_{n=1}^{\infty} \mu(n)/n^s$.
(b) $\zeta(s)^2 = \sum_{n=1}^{\infty} \nu(n)/n^s$.
(c) $\zeta(s)\zeta(s-1) = \sum_{n=1}^{\infty} \sigma(n)/n^s$.

Proof. (a) Using Problem 13 we can write $\zeta(s)^{-1} = \prod_p (1 - (1/p^s))$. If we expand the right hand side we see that we get get a sum of terms $1/n^s$ where n is a squarefree integer. We know n must be squarefree because each prime p appears only once in the product so we will never multiply a prime by itself. Furthermore if n has an odd number of prime factors then the term $1/n^s$ will be negative and if it has an even number of prime factors then it will be positive since terms being multiplied have a $-1/p^s$ term. This explicitly gives the formula $\sum_{n=1}^{\infty} \mu(n)/n^s$.

(b) For some $0 \leq k < s$ we have

$$\zeta(s)\zeta(s-k) = \sum_{u=1}^{\infty} \frac{1}{u^s} \sum_{v=1}^{\infty} \frac{v^k}{v^s} = \sum_{u,v}^{\infty} \frac{v^k}{(uv)^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{uv=n} v^k = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{d|n} d^k.$$

When $k = 0$ we get the formula $\zeta(s)^2 = \sum_{n=1}^{\infty} \nu(n)/n^s$.

(c) This is a special case of the formula in part (b). Putting in $k = 1$ gives $\zeta(s)\zeta(s-1) = \sum_{n=1}^{\infty} \sigma(n)/n^s$. □