4/3 Spring 2025, Number Theory II, Test II practice problems solutions Sitaraman

Howard University Math Department

PLEASE STUDY CLASS NOTES, HW PROBLEMS AND PRACTICE PROBLEMS IN ADDITION TO THESE.

1. True or False ? Prove if true and provide counterexample or disprove if false.

   (a) A unit in a quadratic ring $\mathbb{Z}[\sqrt{d}]$ is always of norm 1.
   False. Take $d = 2$ for a counterexample $1 + \sqrt{2}$ whose norm is -1.

   (b) Every Gaussian integer has a square root that is also a Gaussian integer
   False. Example: square root of $1 + i$ is $\sqrt{\frac{1+\sqrt{2}}{2}} + i\sqrt{\frac{\sqrt{2}-1}{2}}$.

   (c) The equation $x^2 - 7y^2 = -1$ has no solutions in integers. (what about in real numbers?)
   True. $x^2 - 7y^2 = -1 \implies x^2 + 1 = 7y^2$ but a sum of squares of two relatively prime numbers cannot be divisible by a prime that is 3 mod 4, as 7 is.

   (d) The prime 11 is also a Gaussian prime.
   True. 11 is 3 mod 4, so it stays prime in Gaussian integers.

   (e) $3 + i$ is an irreducible (hence prime) Gaussian integer.
   False. $Norm(3 + i) = 3^1 + 1^2 = 10 = 2 \cdot 5$ and using the factors of 2 and 5 we get $3 + i = (2 - i)(1 + i)$ neither of which is a unit.

   (f) For any $n \in \mathbb{Z}$, $n^2 + 1$ is either odd or 2 times an odd number.
   True. If n is even then $n^2 + 1$ is odd. If n is odd, say $n = 2m + 1$, then $n^2 + 1 = 4M + 2 = 2(2M + 1)$ for some M.

   (g) The negative Pell's equation $x^2 - 20y^2 = -1$ has a solution.
   False. From (a) we see that $x^2 + 1 = 20y^2$ is not possible because 20 is not 2 times an odd number.

   (h) If there is no non-trivial solution for $x^p + 9y^p = z^p$ then there is no non-trivial solution for $x^{pk} + 9y^{pk} = z^{pk}$ for any k.
   True. Proof by contrapositive: If there is a non-trivial solution for $x^{pk} + 9y^{pk} = z^{pk}$ then $(x^k)^p + 9(y^k)^p = (z^k)^p$ and this gives a non-trivial solution for $x^p + 9y^p = z^p$.

   (i) If $m^2 + n^2$ is divisible by an odd prime p then $p \equiv 1 \pmod 4$.
   False. This is only guaranteed for m, n that are relatively prime. Take $m = 3, n = 3$ for a counterexample.

2. Prove using properties of a cyclic group of order n that $\sum_{d|n} \phi(d) = n$.

   See notes.

3. If p divides $2^k - 1$ but not for any $n < k$ then show that k divides $p - 1$. In fact show that k divides m for any m for which $2^m \equiv 1 \pmod{p}$.

   Solution: If k is the smallest such that $2^k \equiv 1 \pmod{p}$ means 2 generates a subgroup of $\mathbb{F}_p^*$ of order k and the order of the group is $p-1$. So by Lagrange's theorem k divides $p - 1$.

   To prove the second part let $m = kq + r$ with $r < k$. Then $2^m \equiv 1 \pmod{p}$ means $2^{kq}2^r = (2^k)^q 2^r \equiv 1^q 2^r \equiv 2^r \equiv 1 \pmod{p}$. But this can't happen since k is the order of 2 (least such that $2^k \equiv 1 \pmod{p}$). So that means $r = 0$ and k divides m.

4. Find a fundamental solution and the first three solutions of $x^2 - 7y^2 = 1$.

   Solution:

   $8 + 3\sqrt{7}$ is the fundamental solution and you get the other solutions by taking its powers.

5. Describe the group of units of $\mathbb{Z}[\sqrt{7}]$. (Look at 1c before you answer).

   Solution:

   As shown in 1c the units in this group have to be of norm 1. All of them are generated by $8 + 3\sqrt{7}$. So it is a free group of rank 1.

6. Prove that there are infinitely many square triangular numbers and explain how to produce them.

   Solution:

   Done in text.

7. Describe all the units of $\mathbb{Z}[\sqrt{3}i]$ (Use norm multiplicativity).

   Solution: This is a purely computational problem.

8. Find the greatest common divisor of $5 + 3i$ and $5 + i$. Also find the full factorization into Gaussian primes of the two numbers.

   Solution:

   By factoring the norms, namely 34 and 26, we get that the factors of $5 + 3i$ come from the factors of 2 and 17 and those of $5 + i$ come from the factors of 2 and 13. Actually $5 + 3i = (4 - i)(1 + i)$ and $5 + i = (3 - 2i)(1 + i)$. So the GCD is $1 + i$.

9. (Easy if you get the trick) Show that $x^2 - xy + y^2 = 1$ has only the following solutions in integers, namely $(\pm 1, 0), (0, \pm 1), (1, 1), (-1, -1)$. Note that LHS is the norm of $x + y\rho$ in $\mathbb{Z}[\rho]$ where $\rho = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. So this is saying that the only units in that ring are $\pm 1, \pm\rho, \pm(1 + \rho)$.

Solution:

$$x^2 + y^2 - xy = 1 \implies x^2 + y^2 - 2xy = 1 - xy \implies (x-y)^2 = 1 - xy.$$

Now $(x-y)^2 \geq 0$. So $1 - xy \geq 0$ or $xy \leq 1$. But if x, y are integers, this is only possible if $x = y = 1$ or $x = y = -1$ or one of them is zero or they are of opposite signs. To conclude the proof we only need to look at the case $xy < 0$. (i.e, they are of opposite signs).

In this case we have

$$x^2 + y^2 - xy = 1 \implies x^2 + y^2 = 1 + xy.$$

The LHS is always positive, so this is not possible with $xy < 0$.

BTW $x^2 + y^2 - xy = -1$ is impossible. So the norm cannot be negative in this ring.

$$x^2 + y^2 - xy = -1 \implies x^2 + y^2 + 1 = xy \implies xy > 0.$$
$$x^2 + y^2 - xy = -1 \implies x^2 + y^2 - 2xy = -1 - xy \implies (x-y)^2 = -1 - xy$$
$$\implies -1 - xy \geq 0 \textit{ because } (x-y)^2 \geq 0.$$

But $xy > 0$ and $-1 - xy \geq 0$ are contradictory!

10. Give an example of a negative Pell's equation $x^2 - Dy^2 = -1$ with a fundamental solution. Use it to find two more solutions of that equation as well as three solutions of $x^2 - Dy^2 = 1$.

    Solution:

    $x^2 - 2y^2 = -1$ has fundamental solution $1 + \sqrt{2}$. Odd powers give solutions of the negative Pell's equation and even powers give solutions of the positive Pell's equation.

11. Show that the square root of $3 + 2\sqrt{2}$ is also in $\mathbb{Z}[\sqrt{2}]$ and that the square root of $2i$ is also a Gaussian integer.

    Solution: $1 + \sqrt{2}$ and $1 + i$.

12. Find the number of ways to write 2925 as a sum of two squares.

    Solution:

    This is a purely computational problem, using Legendre's two squares theorem.

13. This is related to the ring of algebraic integers A of $K = \mathbb{Q}[\sqrt{D}]$.

    Reference: K. Conrad's notes on quadratic extensions "Factoring in quadratic fields."

    a) Show that $\mathbb{Z}[\sqrt{D}] \subseteq A$ always and $\mathbb{Z}[\frac{1+\sqrt{D}}{2}] \subseteq A$ if $D \equiv 1 \pmod 4$.

    b) Show that $\mathbb{Z}[\sqrt{D}] = A$ if $D \equiv 3 \pmod 4$ and $\mathbb{Z}[\frac{1+\sqrt{D}}{2}] = A$ if $D \equiv 1 \pmod 4$.

14. This concerns the equation $10^x - y^2 = n$ where x, y, n are positive integers.

    Reference: "Elementary Proof of the Completeness of OEIS A051221 Below 2000" by Seiichi Azuma.

    Show that this can be converted to a Pell type equation (hint: let $x = 2u + 1$).

15. Show that any prime dividing the Fermat number F_n is 1 modulo 4.

    Solution: The Fermat number is a sum of two squares, and the two numbers $2^{2^{n-1}}$ and 1 are relatively prime. So this follows from what we did in the sums of squares section.

16. Show that the Euler function ϕ is multiplicative.

    Solution: This is in the notes / text.

17. If the prime $q \equiv 1 \pmod 4$ and $p = 2q + 1$ is also a prime, show that 2 is a primitive root mod p.

    Solution: If the multiplicative order $o(2)$ in $\mathbb{F}_p^*$ is k then as we saw in 1, it must divide $p - 1$ which equals $2q$. This means $k = 2$ or q. If $k = 2$ then we have $2^2 \equiv 1 \pmod p$ which is not possible here because clearly $p > 3$. If $k = q$ then we have $2^q = 2^{(p-1)/2} \equiv 1 \pmod p$ which by Euler's criterion gives $\left(\frac{2}{p}\right) = 1$. But we know from quadratic reciprocity that this happens only when $p \equiv 1$ *or* $7 \pmod 8$. Here $p = 2q + 1 = 2(4m + 1) + 1 = 8m + 3$. (We got $q = 4m + 1$ because $q \equiv 1 \pmod 4$.

18. Let p be an odd prime and g a primitive root mod p.

    (a) Show that g^k is a quadratic residue mod p iff k is even.

    (b) Using (a) prove Euler's criterion:

$$a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) \pmod p.$$

    Solution: Easy, by looking at the exponents of g. Start by writing $x \equiv g^m$ and then $x \equiv y^2 \pmod p$ will lead to answer if you also note that $y \equiv g^n$ for some n.

19. If (x, y, z) is a solution for $x^4 + y^4 = z^2$ then show that we can use them to produce a solution for $X^2 + 4Y^4 = Z^4$.

    Solution: This is part of the proof of Fermat's last theorem for $n = 4$. It is in the first half of the proof.

20. Compute $\phi(12)$ using only the values of $\phi(1), \phi(2), \phi(3), \phi(4)$ and $\phi(6)$. Then verify your answer using direct computation.

    Use the result $\sum \phi(d) = n$ where d are all the divisors of n.

21. Is it possible to write 1885 as a sum of two squares? As the hypotenuse of a primitive pythagorean triple?

    These are straight applications of theorems in "which numbers are sums of squares"

22. Using the fact that 13 divides $26 = 5^2 + 1$ find a, b such that $13 = a^2 + b^2$.

    Use the same procedure as in descent argument: Start by noting $5 \equiv 1 \pmod 2$ and $1 \equiv 1 \pmod 2$.

$$1^2 + 1^2 = 2 \implies (5^2 + 1^2)(1^2 + 1^2) = 4(13) \implies (5-1)^2 + (5+1)^2 = 4(13).$$

    Now cancelling out 4 on both sides we get $2^2 + 3^2 = 13$.

23. Show that there is only one way to write $p = a^2 + b^2$ with $a \geq b \geq 0$.

    Suppose $a^2 + b^2 = c^2 + d^2 = p$. Then upon multiplying,

$$(a^2 + b^2)(c^2 + d^2) = p^2 \implies (ac - bd)^2 + (ad + bc)^2 = p^2.$$

    From this we get two things. Using Pythagorean triples (they are automatically primitive if p is prime – check!) we get $ac - bd = (s^2 - t^2)/2, ad + bc = st, p = (s^2 + t^2)/2$ from which we get $2p = s^2 + t^2$. On the other hand $a^2 + b^2 \equiv c^2 + d^2 \equiv 0 \pmod p \implies a \equiv \pm b, c \equiv \pm d$. From this we can get that at least one of $ac - bd$ or $ac + bd$ or $ad - bc$ or $ad + bc$ is zero mod p.

    Without loss of generality assume $ac - bd \equiv 0$. Then from $(ac - bd)^2 + (ad + bc)^2 = p^2$ we get that $ad + bc \equiv 0$ also, which means p divides st which contradicts $2p = s^2 + t^2$.