These are homework problems for Math 3600 (Number Theory). Problems will be assigned for each lecture. Please attempt the problems as soon as possible. You will have an opportunity to ask questions about homework on the following Tuesday, and your written solutions will be due two days later on Thursday. For example, the homework assigned for the first two lectures will be due on Thursday **January 16**.

Some of these problems are somewhat open-ended. This gives you an opportunity to explore, experiment, and try to prove as much as you can. Please write your solutions as clearly as possible and with enough detail that another student in the class could follow your reasoning even if they hadn't done the problem themselves.

The acronym *PODASIP* stands for "Prove or Disprove And Salvage If Possible." The given statement may be true or false; you decide which. If it's true, give a proof. If it's false, give a numerical counterexample that shows this. Then try to salvage your false statement by adding a condition or making a similar sounding statement that is in fact true. For extra credit, give a proof that your salvage is correct.

1 Set A

1. Read Silverman: Chapter 1, 4 and pp. 236–240.
2. Without change of base, (a) add $(6153)_7$ to $(3455)_7$; (b) subtract $(2346)_7$ from $(4354)_7$; (c) multiply $(632)_7$ by $(435)_7$; (d) divide $(5602)_7$ by $(5)_7$. Here the base is seven throughout.
3. *In resolving questions and problems posed in the homework, particularly divisibility proofs, one has to make use of many properties of integers. Make a list (inventory) of such properties and see if this inventory suffices for every discussion of questions of arithmetic which we undertake. You can update this on a later homeowork.*
4. *PODASIP:* $a \mid a$ for every $a \in \mathbb{Z}$.
5. *PODASIP:* $a \mid b \Rightarrow b \mid a$ for all a and b in $\mathbb{Z}$.
6. *PODASIP:* For all $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $b \mid c$ then $a \mid c$.
7. *PODASIP:* $a \mid b \Rightarrow a \mid bc$ for all integers a, b, c.
8. *PODASIP:* For all a, b, c in $\mathbb{Z}$, if $a \mid b$ and $a \mid c$ then $a \mid (b + c)$.
9. *PODASIP:* For all $a, b, c \in \mathbb{Z}$, $a \mid bc \Rightarrow a \mid b$ or $a \mid c$.
10. Compute the sum, difference, product, quotient, and remainder of the following two Gaussian integers: $z = 7 - 5i$ and $w = 1 + 2i$. Graph all of the above in the complex plane.

2 Set B

1. Read Silverman Chapter 5
2. Use the Euclidean algorithm to compute each of the following gcd's:
   (a) $\gcd(143, 227)$
   (b) $\gcd(306, 657)$
3. Solve the following linear diophantine equations for integers x and y.
   (a) $56x + 72y = \gcd(56, 72)$
   (b) $24x + 138y = \gcd(24, 138)$
4. *PODASIP:* For all a, b, c in $\mathbb{Z}$, if $a \mid (b + c)$. then $a \mid b$ and $a \mid c$.
5. Use Euclid's algorithm to find the GCD of 29 and 11.
6. Use your work above to show that

$$\frac{29}{11} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3}}}} \; .$$

   This is the *simple continued fraction* for $\frac{29}{11}$.

3 Set C

1. Read Silverman Chapter 6
2. How many of the following can you find in $\mathbb{Z}_7$?

$$4 \cdot 5, \; 2 - 6, \; 1/2, \; 2/5, \; \sqrt{2}, \; \sqrt{-3}, \; \sqrt{-1}, \; \sqrt[3]{6} \; ?$$

   To get you started on this one, let's take a look at the third example: What is $1/2$ in $\mathbb{Z}_7$? To answer this question, we must first realize that $1/2$ stands for the multiplicative inverse of 2 in $\mathbb{Z}_7$. Thus $1/2$ is an element x in $\mathbb{Z}_7$ for which $2x = 1$. Can you find an element $x \in \mathbb{Z}_7$ such that $2x = 1$? Is there more than one such x? Note that $\mathbb{Z}_7$ has has only seven elements. If all else fails, you can always just try out all seven possible values of x.
3. Make an addition table and a multiplication table for the integers $\mathbb{Z}_5$.

4. Find the following elements in $\mathbb{Z}_5$: -1, $1/2$, $2/3$, $\sqrt{-1}$. How many of these elements can you find in $\mathbb{Z}_6$? in $\mathbb{Z}_{10}$? in in $\mathbb{Z}_{13}$?

5. Make a list of the perfect squares in $\mathbb{Z}_5$, in $\mathbb{Z}_{17}$, in $\mathbb{Z}_{19}$, in $\mathbb{Z}_{21}$. How many squares are there in each case? Any conjectures?

6. Solve the following linear equations in one-variable in $\mathbb{Z}_{13}$:

   (a) $2x = 1 \pmod{13}$

   (b) $5x - 7 = 11 \pmod{13}$

   (c) $12x = 9 \pmod{13}$

7. Solve the following linear equations in one-variable in $\mathbb{Z}_{15}$:

   (a) $4x = 11 \pmod{15}$

   (b) $5x = 11 \pmod{15}$

   (c) $9x = 6 \pmod{15}$

8. For which values of a do you think it is possible to solve the quadratic equation $x^2 = a \pmod{13}$? How many solutions will you get?

9. Find all solutions to the quadratic equation $x^2 + 12x - 3 \pmod{15}$. How can you factor this quadratic in $\mathbb{Z}_{15}[x]$?

10. It's interesting to look at powers of numbers in various mods. For example, what do you get if you compute $2^1, 2^2, 2^3, \ldots,$? Can you describe the pattern? Do you get every number in $\mathbb{Z}_5$? What is $2^{2003} \pmod{5}$?

11. What condition on a and b insures that $2^a = 2^b \pmod{5}$?

12. Write each of the following numbers to base three: 3, 9, 27, 243, 1/3, 1/9, 1/27. Write each of these numbers to base two. Any conjectures?

4 Set D

1. Read Silverman Chapter 7–8.

2. Find the GCD of $7+11i$ and $3+5i$ in $\mathbb{Z}[i]$. Does our algorithm in $\mathbb{Z}$ suggest a method?

3. Solve the diophantine equation $(7+11i)X + (3+5i)Y = \gcd(7+11i, 3+5i)$ in $\mathbb{Z}[i]$.

4. *PODASIP:* $ac = bc \Rightarrow a = b$. True in $\mathbb{Z}$. True in $\mathbb{Z}_m$.

5. Make a table of the powers of 2 and the powers of 3 in $\mathbb{Z}_{17}$. What patterns do you notice?

6. Can you use your table to help you find all the solutions in $\mathbb{Z}_{17}$ to the following equations.

   (a) $x^5 = 6$.

   (b) $3x^6 = 7$

7. Write down all the elements of U_7, of U_{15}, of U_{18}, of U_{21}. Which of these are cyclic? Any conjectures?

8. Construct a table of "logarithms" (indices) for U_{17}. This is just the inverse table for a power table in U_{17}.