COURSE DIGEST, MATH 601, SPRING 2026

Week 02 01/27 and 01/29

Read HPS: 1.2, 1.3

Exercises HPS: 1.9, 1.10, 1.11

Tuesday Borrowing from linear algebra, we introduced the concept of a $\mathbb{Z}$-linear combination of integers $x_1, \ldots, x_n$, and also the $\mathbb{Z}$-span $\operatorname{span}_{\mathbb{Z}}(x_1, \ldots, x_n)$. We went over lots of examples, and described the **Extended Euclidean Algorithm (EEA)**.

Thursday We stated the **Bezout Identity**: If a, b are positive integers, then there exist $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$. We then obtained the **Corollary**: If $a, b \in \mathbb{Z}$, then $\operatorname{span}_{\mathbb{Z}}(a, b) = \operatorname{span}_{\mathbb{Z}}(\gcd(a, b)) = \{0, \pm \gcd(a, b), \pm 2 \gcd(a, b), \ldots, \}$. We discussed how this means that $\gcd(a, b)$, which is supposed to be great, is the *least* positive integer in the span of a and b. After this, we introduced the term *relatively prime* for integers, went over examples, and proved some basic facts. We ended the lecture by introducing modular arithmetic, and covered some basic properties.

Week 01 01/20 and 01/22

Read Secure a copy of Hoffstein, Pipher, Silverman (HPS).

Exercises $\varnothing$.

Tuesday Welcome to MATH 601! We spent most of lecture on introductions and the syllabus. Math-wise, we introduced basic notation and presented the **Well-ordering Principle**, which states that any non-empty subset of $\mathbb{N}$ contains a least element. More math next time!

Thursday We started by recalling the Well-ordering Principle, and used it to prove that $\sqrt{2} \notin \mathbb{Q}$. We then used WO to prove the **Division Algorithm**: If $a, b \in \mathbb{N}$ with $a \neq 0$, then there exist unique $q, r \in \mathbb{N}$ with $0 \leq r < a$ such that $b = aq + r$. We then defined what it means for an integer to divide another, and defined the greatest common divisor of two integers. We proved that if a, b are as above, then $\gcd(a, b) = \gcd(a, r)$ and saw how to iterate this to effectively compute gcds.