Contents

2 Class Lecture 9/25

Def^n: Prime
Def^n: Relatively Prime

Axiom: For any non-zero ratio r=$\frac{p}{z}$, where $p, z \in \mathbb{Z}$, p and q are relatively prime.
Thm. 2.2.2: $\sqrt{2}$ is irrational.

Proof:

1. By contradiction. Assume $\sqrt{2}$ is rational.
2. $\therefore$ $\sqrt{2} = \frac{p}{z}$, where p and q are relatively prime.
3. $\left(\sqrt{2}\right)^2 = (p)^2$
4. $\left(\sqrt{2}\right)^2 (q)^2 = (p)^2$
5. $2q^2 = p^2$
6. $\therefore$ p^2 is even. What does tat about p?
7. Because odd odd = odd, p must be even
8. $\therefore$ $2|p$, so $p = 2k$ for some $k \in U$
9. $2q^2 = (2k)^2 \to 2q^2 = 4k^2 \therefore q^2 = 2k^2$
10. By the same arguments as above, q is even $\therefore$ $2|q$. So $2|p$ and $2|q$.
11. Hence, p and q are not relatively prime. So p and q are relatively prime and p and q are not relatively prime.
12. $\therefore$ Our assumption that $\sqrt{2}$ is ratiional must be false; i.e. $\sqrt{2}$ is irrational. **QED**

Thm: There are irrational numbers r, s so that r^s is rational.

Proof

1. Consider $r = \sqrt{2}$ and $s = \sqrt{2}$. Look at $r^s = \sqrt{2}^{\sqrt{2}}$
   (a) $\sqrt{2}^{\sqrt{2}}$ is rational. Done this case! $r = p$ and $s = q$
   (b) $\sqrt{2}^{\sqrt{2}}$ is irrational: Consider $r = \sqrt{2}^{\sqrt{2}}$ and $s = \sqrt{2}$. Double rational needs fixing

More Skipping Around

Axiom: Well-Ordering Princple – Every non-empty subset of $\mathbb{N}$ contains a least element

$$\forall A \subseteq \mathbb{N} [\ A \neq \emptyset \to \exists x \in A\, (\forall X \in A\, (x <= y))\ ]$$

Thm 2.2.4 Every natural number > 1 is divisible by some prime.

$$\forall n \in \mathbb{N}\, (n > 1 \to \exists p \in \mathbb{N}\, (pisprimeandp|n))$$

Proof:

1. Let $n \in \mathbb{N}$. Assume $n > 1$.
2. Case 1: n is prime.
   (a) $n|n$, because $n = n \times 1$. Done
3. Case 2: n is composite.
   (a) $\therefore n$ has a non-trivial divisor
   (b) $\therefore$ there is a d such that $1 < d < n$ and $d|n$
   (c) Let $A = \{x|1 < x < n \ and\ x|n\}$
   (d) So $d \in A\ \ \therefore A \neq \emptyset$

Quiz 2 Review

3b. $\exists x \in D\, (\forall y \in U\, (f(\pi y) = 0))$

2 Class Lecture 9/28

Well-Ordering Principle

Theorem 2.1 (Well Ordered Principle)**.** $\forall n \in \mathbb{N}(n > 1 \to \exists p \in \mathbb{N}(p \textit{ is prime } \wedge p|n))$

Proof. Let $n \in \mathbb{N}$. Assume $n > 1$. **Case 1:** n is prime. $n|n$ ✓. **Case 2:** n is not prime. $\exists\ d\ \mathbb{N}((1 < d < n) \wedge (d|n))$. A is of the form $A = \{x|(1 < x < n) \wedge (x|n)\}$. $A \neq \emptyset$ because $d \subset A$. By the Well Ordering Principle A has a least element $d^* \in A$. $\therefore$ $(1 < r^* < n) \wedge (r^*|n)$. **Claim:** r^* is prime. □

Proof:

1. Let $n \in \mathbb{N}$. Assume $n > 1$
   (a) f
      i. Proof of Claim: by Contradiction.
         A. Assume r^* is not prime.
         B. $\therefore$ there is an s within $1 < s < r^*$ such that $s|r^*$.
         C. So $1 < s < r^* < n$ and $s|r^*$ and $r^*|n$.
         D. Hence $1 < s < n$ and $s|n$.
         E. $s \in A$ and $s < r^*$, the least element of A
         F. $\therefore$ r^* must be prime, **QED** for claim.
   (b) $r^*|n$ and r^* is prime. Hence n has a prime divisor **QED**.

There are infinitely many primes..

Thm. 2.2.5 There are infinitely many primes.
Proof: By Contradiction

1. Assume $p_1, p_2, ..., p_k$ is a finite list of **all** the primes.
2. Let $n = p_1 \times p_2 \times p_3 \times ... \times p_k + 1$. $n > p_i$ for all primes.
3. $\therefore$ n is not prime.
4. However, n is divisible by a prime. $\therefore$ for some $i \leq k$, $p_i|n$.
5. Call $p_1, p_2, ..., p_k = m$
6. So $n = m + 1$, and $p_i|n$, so $n = p_i q$ for some $q \in \mathbb{Z}$
7. $pi|m$ because $m = p_i(p_1 p_2, ..., p_{i-1}, p_{i+1}, ...p_k)$
8. $n = m + 1$, $p_i q = p_i(t) + 1$, hence $1 = p_i \underbrace{(q - t)}_{\in \mathbb{Z}}$
9. **QED**

Induction

Proving "$\forall$ statement" about a well-ordered set.

Idea:

Setting: Want to prove $\forall n \in \mathbb{N}\left(n \geq a \rightarrow \underbrace{P(n)}_{some\ statement}\right)$

Proof: Base case

1. Prove $P(a)$ is true.
2. **Induction Step** $\rightarrow \forall k \in \mathbb{N}((k \geq a \wedge P(k)) \rightarrow P(k+1))$: Assume $k \geq a \wedge P(k)$
   (a) From this assumption, prove $P(k+1)$

Prove:

$$\forall n \in \mathbb{N}(0+1+...+n = \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$

1. Proof by induction. Base Case: $n = 0$.
2. Induction Step: Let $k \geq 0$ and assume $\sum_{i=0}^{n} i = \frac{k(k+1)}{2}$
   (a) To Show: $\sum_{i=0}^{k+1} i = 0+1+2+...+k+(k+1) = \frac{(k+1)((k+1)+1)}{2}$
3. sumation = (k(k+1))/2 + (k+1) = (k+1)(k/2 + 1) = (k+1)(k/2 + 2/2) = (k+1)((k+2)/2) = (k+1)((k+1)+1)/2 QED