

Course Notes for Math 320:
Fundamentals of Mathematics
Homework Hints for Number Theory.

October 5, 2005

88 Let r_1, r_2, r_3, \dots be an infinite sequence of nonnegative integers such that $r_1 > r_2 > r_3 > \dots$. Prove that for some number $k \in \mathbf{N}$, $r_k = 0$.

Hint:

- (a) Let $S = \{r_1, r_2, r_3, \dots\}$.
- (b) To get a contradiction suppose that for every k we have that $r_k \neq 0$.
- (c) Then $S \subset \mathbf{N}$ (why?).
- (d) Now use LNNP to show that there is a least element of S .
- (e) Finally show that having a least element in S contradicts the given fact that $r_1 > r_2 > r_3 > \dots$

103(a) Let a and b be integers not both 0, and let $d = \gcd(a, b)$ then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Hint:

- (a) Let $m = \gcd(\frac{a}{d}, \frac{b}{d})$.
- (b) Show that there exist $x, y \in \mathbf{Z}$ such that $mx = \frac{a}{d}$ and $my = \frac{b}{d}$.
- (c) Use this to show that $md|a$ and $md|b$.
- (d) Use this and the fact that $d = \gcd(a, b)$ to show that $md \leq d$.
- (e) Use this to show that $m = 1$.

103(b) Let a and b be integers not both 0, and let $d \in \mathbf{N}$ be such that $d|a$ and $d|b$. If $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$ then $\gcd(a, b) = d$.

Hint: We will show that $d|(\gcd(a, b))$ and $\gcd(a, b)|d$.

- (a) We have that $d|a$ and $d|b$ and that $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.
- (b) We showed (when?) that this implies that $d|\gcd(a, b)$.
- (c) Now we are assuming that $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$. Use this to show that there is a solution to the diophantine equation $(\frac{a}{d})x + (\frac{b}{d})y = 1$.
- (d) Manipulate this equation to show that there is a solution to $ax + by = d$.

(e) Use the theorem from Wednesday to show that this implies that $\gcd(a, b) | d$.

113 Show that there are infinitely many primes of the form $6n + 5$. Hints:

- Let $W = \{n \in \mathbf{N} \mid \exists q \in \mathbf{Z} \text{ with } n = 6q + r \text{ where } r = 0, 1, 2, 3, \text{ or } 4\}$. These are the numbers not having remainder 5 when divided by 6. Show that if $n, m \in W$ then $nm \in W$.
- Suppose that there are not infinitely many primes greater than 5 of the form $6n + 5$. Then there exists an $n \in \mathbf{N}$ such that $\{p_1, p_2, \dots, p_n\}$ are all the primes greater than 5 of this form. Let $M = p_1 p_2 \dots p_n$ and let $N = 6M + 5$. Suppose that $p = 6k + 5$ is a prime show that $p \nmid N$.
- Explain why N must be the product of prime numbers none of which has remainder 5 when divided by 6.
- Explain why this implies that N does not have a remainder of 5 when divided by 6.
- What does this contradict?

101 Consider the set $S = \{n \in \mathbf{N} \mid \text{if } a_1, a_2, \dots, a_n \in \mathbf{Z} \text{ and } p \text{ a prime such that } p | a_1 a_2 \dots a_n \text{ then } p | a_i \text{ for some } i \in \{1, 2, \dots, n\}\}$

103 For the direction \Leftarrow , suppose that $d = \gcd(a, b)$ and $m = \gcd(\frac{a}{d}, \frac{b}{d})$. Show that there exist $x, y \in \mathbf{Z}$ such that $mx = \frac{a}{d}$ and $my = \frac{b}{d}$. Use this to show that $m = 1$.

For the converse direction: We have that $d | a$ and $d | b$ and that $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$. Using the definition of gcd show that $d | \gcd(a, b)$. Use that $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$ to show that there is a solution to the diophantine equation $x(\frac{a}{d}) + y(\frac{b}{d}) = 1$. Manipulate this to show that $\gcd(a, b) | d$.

111 The possibilities for p , q , and r are numbers of the form $5l + r$ where r is 0, 1, 2, 3, or 4. Think of what happens when you square them... what are the possible remainders when you divide the squares by 5? Then add them up.

112 Note that if A and B are natural numbers having remainder 1 when divided by 4 then so does AB (proof?). Mimic the proof that there are infinitely many primes: That is, suppose that there are only finitely many prime numbers greater than 3 of the form $4k+3$ and let M be their product.

Groupwork: Prove that there exist infinitely many primes.

Hints:

- Suppose not. Then there exists an $n \in \mathbf{N}$ such that $\{p_1, p_2, \dots, p_n\}$ is all the primes. Let $N = p_1 p_2 \dots p_n + 1$. Prove that there exists a prime p such that $p | N$.
- Show that $p = p_i$ for some $i = 1, 2, \dots, n$ so $p | (p_1 p_2 \dots p_n)$.
- Show that $p | 1$.
- Show why this is a contradiction.