

Math 111, HW 2

Curtis Paul

April 23, 2007

15. If a is a square, let b be a square root of a . For each prime p , $\text{ord}_p(a) = 2 \text{ord}_p(b)$, so $\text{ord}_p(a)$ is even.

If $\text{ord}_p(a)$ is even for all primes p , let

$$b = \prod_p p^{\frac{\text{ord}_p(a)}{2}}.$$

Then $b^2 = a$, as desired.

In general, a is an n^{th} power if and only if $\text{ord}_p(a)$ is a multiple of n for all primes p .

19. $|ab|$ is a common multiple, so there is a common multiple, m , least in size. If n is a common multiple of a and b , (m, n) is a common multiple of a and b . m is the smallest such, so $m = (m, n)$ implies $m \mid n$.

20. a) $a \mid [a, b]$, $b \mid [a, b]$, so $\text{ord}_p a \leq \text{ord}_p[a, b]$, $\text{ord}_p b \leq \text{ord}_p[a, b]$, so $\max(\text{ord}_p a, \text{ord}_p b) \leq \text{ord}_p[a, b]$.

$$\prod_p p^{\max(\text{ord}_p(a), \text{ord}_p(b))}$$

is a common multiple of a and b , so $\text{ord}_p[a, b] \leq \max(\text{ord}_p a, \text{ord}_p b)$ implies $\text{ord}_p[a, b] = \max(\text{ord}_p a, \text{ord}_p b)$.

b) $\text{ord}_p(a, b)[a, b] = \text{ord}_p(a, b) + \text{ord}_p[a, b] = \min(\text{ord}_p a, \text{ord}_p b) + \max(\text{ord}_p a, \text{ord}_p b) = \text{ord}_p a + \text{ord}_p b = \text{ord}_p ab$, so $(a, b)[a, b] = ab$.

c) $\text{ord}_p(a + b, [a, b]) = \min(\text{ord}_p(a + b), \text{ord}_p[a, b]) = \min(\text{ord}_p(a + b), \max(\text{ord}_p a, \text{ord}_p b))$. If $\text{ord}_p a = \text{ord}_p b$, $\text{ord}_p(a + b) \geq \text{ord}_p a$ implies $\min(\text{ord}_p(a + b), \max(\text{ord}_p a, \text{ord}_p b)) = \text{ord}_p a = \min(\text{ord}_p a, \text{ord}_p b) = \text{ord}_p(a, b)$. If $\text{ord}_p a > \text{ord}_p b$, $\text{ord}_p(a + b) = \text{ord}_p b$, so $\min(\text{ord}_p(a + b), \max(\text{ord}_p a, \text{ord}_p b)) = \text{ord}_p b = \text{ord}_p(a, b)$. Similarly for $\text{ord}_p a < \text{ord}_p b$. $\text{ord}_p(a + b, [a, b]) = \text{ord}_p(a, b)$ implies $(a + b, [a, b]) = (a, b)$.

23. Without loss of generality, a is even and b and c are odd. Look mod 4 to see this. $a^2 = c^2 - b^2 = (c - b)(c + b)$. If m divides $c - b$ and $c + b$, it divides their sum and difference, so $m \mid 2c$ and $m \mid 2b$. $(b, c) = 1$, so m is 1 or 2. $c - b$ and $c + b$ are even, so $(c - b, c + b) = 2$. For primes p , $p > 2$, $\text{ord}_p a$ is even. Either $\text{ord}_p(c - b) = 0$ or $\text{ord}_p(c + b) = 0$, so $\text{ord}_p(c - b)$ and $\text{ord}_p(c + b)$ are even. $\frac{c-b}{2}$ and $\frac{c+b}{2}$ are relatively prime, so similarly to the above, $\text{ord}_2(\frac{c-b}{2})$ and $\text{ord}_2(\frac{c+b}{2})$ are even. This means that $c - b = 2v^2$ and $c + b = 2u^2$ with $(u, v) = 1$. The other direction is straight calculation.

26. If $a^n + 1$ is an odd prime, a^n is even, so a is even. If n has an odd prime factor, p , $a^n + 1 = (a^k)^p + 1$, which is a sum of p powers and hence factorable, which is a contradiction.

27. Check mod 8 and mod 6.

30.

$$\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} = \frac{\frac{n!}{2} + \frac{n!}{3} + \cdots + \frac{n!}{n}}{n!}.$$

Let 2^m be the largest power of 2 less than or equal to n . For all terms in the numerator except $\frac{n!}{2^m}$, $\text{ord}_2(\frac{n!}{k}) > (\text{ord}_2(n!)) - m$, so the order at 2 of the sum of all those terms is greater than $(\text{ord}_2(n!)) - m$. But this is the order of the term $\frac{n!}{2^m}$, so the order at 2 of the entire numerator is $(\text{ord}_2(n!)) - m$. This is less than the order at 2 of the denominator, so the sum is not an integer.