

Solutions/ Hints to homework 2

January 11, 2008

21 and 22. Let's do only 21, as 22 is similar. Let S_1 be the set of all common divisors of a and $a + b$, let S_2 be the set of all common divisors of a and b . Show that $S_1 = S_2$ (see also the proof of Lemma 1.7, page 12). Therefore the largest element in S_1 (i.e. $(a, a + b)$) is the same as the largest element in S_2 (i.e. (a, b) .)

25. Let's do the inductive step. We assume that $(a, b^n) = 1$ and we try to show that $(a, b^{n+1}) = 1$. Write $1 = xa + yb^n$. Then $1 = (xa + yb^n)^2 = (x^2a + 2xyb^n)a + (y^2b^{n-1})b^{n+1}$.

26. Let $d = (a, b)$. Assume first that the given equation has integer solutions, i.e. $c = ax + by$ for some integers x and y . We know $d|a$ and $d|b$ hence $d|(xa + yb)$. Assume now that $d|c$. Then $c = dz$ for some integer z . Write $d = ma + nb$, where m, n are integers. Then $c = dz = (mz)a + (nz)b$, hence the given equation has integer solutions.

31. a) Assume that k does not divide $[a, b]$. Then $k = [a, b]q + r$, $0 < r < [a, b]$. Since $a|k$ and $a|[a, b]$ we get that $a|r$. For same reason $b|r$. Therefore r is a common multiple, hence $[a, b] \leq r$. Contradiction.

b) Note that $a|\frac{ab}{(a,b)}$ (to see that write $\frac{ab}{(a,b)} = a \cdot \frac{b}{(a,b)}$ and recall that $(a, b)|b$). Similarly, $b|\frac{ab}{(a,b)}$. By part a) we get that $[a, b]|\frac{ab}{(a,b)}$.

Now we will show $\frac{ab}{(a,b)}|[a, b]$. Write $[a, b] = q\frac{ab}{(a,b)} + r$, $0 \leq r < [a, b]$. Assume that $r \neq 0$. But then $a|r$ and $b|r$ (since both a and b divide $[a, b]$ and $\frac{ab}{(a,b)}$) and r is smaller than the least common multiple. Contradiction.

32. Consider an integer z . Write $z = a_n 10^n + \dots + 10a_1 + a_0$. Note that $10^k - 1 = 9 \dots 9 = 3 \cdot 3 \dots 3$, i.e. $10^k - 1$ is divisible by 3. Write $z = a_n(10^n - 1) + a_n + \dots + (10 - 1)a_1 + a_1 + a_0 = (a_n(10^n - 1) + \dots + (10 - 1)a_1) + (a_n + \dots + a_1 + a_0)$. The first summand (i.e. $(a_n(10^n - 1) + \dots + (10 - 1)a_1)$) is divisible by 3, hence z is divisible by 3 iff $(a_n + \dots + a_1 + a_0)$ is.

34. a) $(a, b)|a$, $(a, b)|b$, hence $(a, b)|(a \pm b)$, hence $(a, b)|(a + b, a - b)$, by Cor.1.4.

b) Apply part a) to get that $(a + b, a - b)|((a + b) + (a - b), (a + b) - (a - b))$, i.e. $(a + b, a - b)|(2a, 2b)$, i.e. $(a + b, a - b)|2(a, b)$. Now, since $a + b$ and $a - b$ are odd, we get that $((a + b, a - b), 2) = 1$ (I know, it does look confusing). By Thm.1.5 we have that $(a + b, a - b)|(a, b)$. Combine it with part a) and the fact that gcd is always positive.

c) same story as part b).