Math 215, Fall 05 Homework #12 Solution

12/02/05

1. (**20 points total**) d, a, b, r, q are integers.

a) Since $d|a$ and $d|b$ there are integers x and y such that $xd = a$ and $yd = b$. Therefore

$$ra + sb = r(xd) + s(yd) = (rx)d + (sy)d = (rx + sy)d$$

which means $d|(ra + sb)$. (**8 points**)

b) $a = qb + r$. Suppose that $d|a$ and $d|b$. Then $d|(1a + (-q)b)$ by part a). Thus $d|r$. We have shown that a divisor of a and b is a divisor of r and is thus a divisor of b and r. (**6 points**)

Conversely, suppose $d|b$ and $d|r$. Then $d|(qb + 1r)$ by part a). Thus $d|a$. We have shown that a divisor of b and r is a divisor of a and is thus a divisor of a and b. (**6 points**)

2. (**20 points total**) By Problem 1 the set of common divisors of a and b is the set of common divisors of b and r. Therefore $\gcd(a, b) = \gcd(b, r)$. Part b) is a direct consequence of this equation. (**12 points**)

Suppose $r = 0$. Since $\mathbf{Z}$ is the set of divisors of 0, the set of common divisors of b and r is the set of divisors of b. Since $b > 0$ it follows that the greatest integer among the divisors of b is b itself. Thus part a) follows. (**8 points**)

3. (**20 points total**) Problem 2 is to be applied.

a) $a = 100$ and $b = 3$. Since $100 = 33{\cdot}3 + 1$ we conclude $\gcd(100, 3) = \gcd(3, 1) = 1$. (**5 points**)

b) $a = 100$ and $b = 82$. The calculations

$$\begin{aligned} 100 &= 1{\cdot}82 + 18 \\ 82 &= 4{\cdot}18 + 10 \\ 18 &= 1{\cdot}10 + 8 \\ 10 &= 1{\cdot}8 + 2 \\ 8 &= 4{\cdot}2 + 0 \end{aligned}$$

show that

$$\gcd(100, 82) = \gcd(82, 18) = \gcd(18, 10) = \gcd(10, 8) = \gcd(8, 2) = 2.$$

(**15 points**)

4. (**20 points total**) This is a bit of a challenge. Part a) makes the technical details easy. Our basic premise is p and a are positive integers and $p|a^2$.

a) Since $p|a^2$ there is an integer x such that $xp = a^2$. Thus for integers r, s the calculation

$$\begin{aligned}(ra + sp)^2 &= (ra)^2 + 2(ra)(sp) + (sp)^2 \\ &= r^2a^2 + 2rasp + s^2p^2 \\ &= r^2xp + 2rasp + s^2p^2 \\ &= (r^2x + 2ras + s^2p)p\end{aligned}$$

shows that $p|(ra + sp)^2$. (**5 points**)

b) We prove the assertion $p|a^2$ implies $p|a$ by induction on a (the strong induction principle is used). The case $a = 1$ is vacuous since $p \not| 1^2$. Thus the conclusion is true for $a = 1$ (that is $p|1^2$ implies $p|1$).

Suppose that $a > 1$ and $p|b^2$ implies $p|b$ is true for all $1 \leq b < a$. Suppose $p|a^2$.

Case 1: $a \leq p$. By Theorem 15.1.1 there are integers q, r such that $p = qa + r$ and $0 \leq r < a$. Since $r = (-q)a + 1p$ we conclude that $p|r^2$ by part a). Thus $p|r$ by our induction hypothesis. If $r \neq 0$ then $p \leq r$ since $0 \leq r$. But then $r < a \leq p \leq r$, a contradiction. Therefore $r = 0$ which means $p = qa$. Since p is prime and $a \geq 1$ necessarily $a = 1$ or $a = p$. The former is not possible since $p|a^2$. Thus $p = a$ which means $p|a$.

Case 2: $a \not\leq p$ or equivalently $p < a$. By Theorem 15.1.1 there are integers q, r such that $a = qp + r$ and $0 \leq r < p$. Since $r = (-q)p + 1q$ it follows by part a) again that $p|r^2$. Now $0 \leq r < p < a$ means $p|r$ by the induction hypothesis. Therefore $p|(qp + 1r)$ by part a) of Problem 1, or $p|a$.

We have shown that if $a > 1$ and the induction hypothesis is true for $1, \ldots, a - 1$ then it is true for a. Since the assertion is true for $a = 1$, by the strong induction principle the assertion is true for all $a \geq 1$. (**15 points**)