

HOMEWORK 5
Math 109 - Dr. Chow
UCSD Winter 2003

92. Let b be a nonzero integer and let a, q, r be integers such that $a = bq + r$. Prove that $\gcd(a, b) = \gcd(b, r)$.

To show that the two gcd's are the same, we show that each one divides the other, since $m|n$ and $n|m$ means that $m = n$. By Theorem 3.9, $\gcd(a, b)$ divides by a and b , and if c also divides both a and b , then c also divides $\gcd(a, b)$.

First, $\gcd(b, r)$ divides both b and r , so it also divides $a = bq + r$. Hence, $\gcd(b, r) | \gcd(a, b)$. Likewise, $\gcd(a, b)$ divides both a and b , so it divides $r = a - bq$. This shows that $\gcd(a, b) | \gcd(b, r)$. We conclude that $\gcd(a, b) = \gcd(b, r)$. \square

98. Prove Corollary 3.11: If a, b , and c are integers such that a and b are relatively prime and $a|bc$, then $a|c$.

Suppose that a and b are relatively prime and $a|bc$. By definition of relatively prime, $\gcd(a, b) = 1$. By Theorem 3.10, we can find integers m and n such that $1 = ma + nb$. Multiplying both sides by c , we get $c = mac + nbc = (mc)a + n(bc)$. a clearly divides $(mc)a$, and a divides $n(bc)$ by assumption. Thus, a divides $(mc)a + n(bc) = c$, as desired. \square .

106. Let a, b and c be integers such that $\gcd(a, c) = \gcd(b, c) = 1$. Prove that $\gcd(ab, c) = 1$.

I will give two proofs, the first by contradiction and the second by a smooth trick. Assume for sake of contradiction that $\gcd(a, c) = \gcd(b, c) = 1$ but $\gcd(ab, c) \neq 1$. This means that $d = \gcd(ab, c) > 1$, so there is a prime number p that divides d . By definition, d divides both ab and c , which means that p divides by ab and c . By Corollary 3.13 (or Exercise 100), p divides ab implies that either p divides a or p divides b . If p divides a and p divides c , this contradicts $\gcd(a, c) = 1$. If p divides b and p divides c , this contradicts $\gcd(b, c) = 1$. In either case, we have a contradiction, and therefore $\gcd(ab, c)$ must be 1. \square

Here is a clever way of showing the same thing. Since $\gcd(a, c) = 1$, there are integers m and n such that $ma + nc = 1$. Likewise, there exist integers r and s such that $rb + sc = 1$. Here's the trick: multiply the two equations together.

$$\begin{aligned}(ma + nc)(rb + sc) &= 1 \\ mrab + msac + nrbc + nsc^2 &= 1 \\ (mr)ab + (msa + nr b + nsc)c &= 1\end{aligned}$$

mr and $msa + nr b + nsc$ are both integers, so 1 is an element of the set $S = \{m(ab) + nc : m, n \in \mathbf{Z}\}$. By Theorem 3.10, $\gcd(ab, c)$ is the smallest natural number belonging to S , which must be 1. We conclude that $\gcd(ab, c) = 1$. \square