

1. (0.10) Let $d = \gcd(a, b)$. If $a = da'$ and $b = db'$, show that $\gcd(a', b') = 1$.

Proof. Since $d = \gcd(a, b)$, there exists integers s and t such that

$$d = as + bt.$$

This can be rewritten as

$$d = da's + db't.$$

Dividing each side by d gives $1 = a's + b't$. Any number that divides both a' and b' would divide 1. Hence $\gcd(a', b') = 1$.

2. (0.14) Show that $5n + 3$ and $7n + 4$ are relatively prime for all n .

Proof. First observe that for any n ,

$$7(5n + 3) - 5(7n + 4) = 35n + 21 - 35n - 20 = 1.$$

Hence any number that divides both $5n + 3$ and $7n + 4$ also divides 1. Thus the two numbers are relatively prime.

3. (0.30) Show that $n \equiv n^3 \pmod{6}$ for all $n > 0$.

Proof. We have to show that $6|n^3 - n$ for all $n > 1$. But $n^3 - n = n(n^2 - 1) = n(n-1)(n+1)$. Thus $n^3 - n$ is the product of three consecutive integers - $n-1, n, n+1$. Clearly one of these numbers must be even, hence one is divisible by 2. Also the difference of any two of these numbers is either ± 1 or ± 2 . Therefore the numbers are distinct mod 3. Thus the remainders when dividing by 3, take on the values 0, 1, 2. In particular, one of these numbers is divisible by 3. Hence $n^3 - n$ is divisible by both 2 and 3. Since 2 and 3 are relatively prime, $n^3 - n$ is divisible by their product, namely 6.

4. (2.34) Show that the given set of 3×3 matrices is a group.

Proof. The multiplication that is defined in the problem is just ordinary matrix multiplication. Hence it is clear that the operation is associative (don't have to prove). It is also clear from the definition given in the book, that the product of two elements in the set (i.e., each is upper triangular with 1's on the main diagonal) is again in the set. So the set is closed under the operation. Moreover, the 3×3 identity matrix is the identity element for this operation and this lives in the set (where $a = b = c = 0$). The only thing we need show is that inverses of elements in the set exist and are in the set.

We need to know that the inverse of a matrix

$$A = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

has the same form, namely upper triangular with 1's on the main diagonal.

There are a number of methods of computing the inverse of a matrix, including row reducing the augmented matrix $(A|I)$. One finds that

$$A^{-1} = \begin{bmatrix} 1 & -a & ac - b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix}.$$

Clearly this has the appropriate form (i.e., upper triangular with 1's on the main diagonal), so it is an element of the set. Hence the set is a group.