Algorithmic Foundations 2 - Tutorial Sheet 4

Integers and Matrices

---

1. Applying the division algorithm with $a = -35$ and $d = 6$ yields what value of r?

> **Solution:** The answer 1 since $-35 = 6{\cdot}(-6) + 1$. Recall that we must find q and r such that $0 \leq r < 6$.

2. Find:

   (a) $\gcd(20!, 12!)$;

   > **Solution:** We have that 12! divides itself and 20! (since $20! = 12!{\cdot}13{\cdot}14{\cdot}15{\cdots}19{\cdot}20$), and hence $\gcd(20!, 12!) = 12!$.

   (b) $\gcd(289, 2346)$;

   > **Solution:** Using the Euclidean algorithm:
   >
   > $$\begin{aligned} 2346 &= 289{\cdot}8 + 34 \\ 289 &= 34{\cdot}8 + 17 \\ 34 &= 17{\cdot}2 + 0 \end{aligned}$$
   >
   > and therefore $\gcd(2346, 289) = 17$

   (c) $\mathrm{lcm}(20!, 12!)$;

   > **Solution:** For similar reasoning to part (a) we have $\mathrm{lcm}(20!, 12!) = 20!$

   (d) $\mathrm{lcm}(289, 2346)$.

   > **Solution:** Computing the prime factorisations, first 289 is not divisible by 2, 3, 5, $\ldots$, 13, nor 15 and $289/17 = 17$, it follows that $289 = 17^2$. Considering the prime factorisation of 2346 we have:
   >
   > - $2346/2 = 1173$ and 1173 is not divisible by 2;
   > - $1173/3 = 391$ and 391 is not divisible by 3, 5, 7, 9, 11, nor 13;
   > - $391/17 = 23$ and $\sqrt{23} < 17$
   >
   > and hence $2346 = 2^1{\cdot}3^1{\cdot}17^1{\cdot}23^1$.
   > Combining these results with the approach for computing lcms explained in the lectures, it follows that $\mathrm{lcm}(289, 2346) = 2^1{\cdot}3^1{\cdot}17^2{\cdot}23^1 = 39882$.

3. List all positive integers less than 21 that are relatively prime to 33.

> **Solution:** The number p is relatively prime to 33 if $\gcd(p, 33) = 1$, hence the relatively prime positive integers less than 21 are: 1, 2, 4, 5, 7, 8, 10, 13, 14, 16, 17, 19, 20

4. Find:
   (a) 18 mod 7

   > **Solution:** Using the division algorithm we have $18 = 7{\cdot}2{+}4$, and hence $18 \bmod 7 = 4$

   (b) $-88 \bmod 13$

   > **Solution:** Using the division algorithm we have $-88 = 13{\cdot}(-7) + 3$, and hence $18 \bmod 7 = 3$

   (c) 289 mod 17

   > **Solution:** Using the division algorithm we have $289 = 17{\cdot}17{+}0$, and hence $289 \bmod 17 = 0$

5. Determine whether each of the following 'theorems' is `true` or `false`. Assume that a, b, c, d and m are integers with $m{>}1$.
   (a) If $a \equiv b \pmod{m}$, and $a \equiv c \pmod{m}$, then $a \equiv b + c \pmod{m}$

   > **Solution:** `false` - for example considering $a = b = 1$, $c = 3$ and $m = 2$, then:
   >
   > - $1 \equiv 1 \pmod{2}$ since 2 divides $1{-}1 = 0$ 2;
   > - $1 \equiv 3 \pmod{2}$ since 2 divides $1{-}3 = -2$ 2;
   > - $1 \not\equiv 4 \pmod{2}$ since 2 does not divide $1{-}4 = -3$.

   (b) If $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$, then $a{\cdot}c \equiv b{+}d \pmod{m}$

   > **Solution:** `false` - for example, considering $a = 0$, $b = 2$, $c = 1$, $d = 1$ and $m = 2$, then
   >
   > - $0 \equiv 2 \pmod{2}$ since 2 divides $0{-}2 = -2$;
   > - $1 \equiv 1 \pmod{2}$ since 2 divides $1{-}1 = 0$;
   > - $0 \not\equiv 3 \pmod{2}$ since 2 does not divide $0{-}3 = -3$.

   (c) If $a \equiv b \pmod{m}$, then $2{\cdot}a \equiv 2{\cdot}b \pmod{m}$

   > **Solution:** `true` - if m divides $a - b$, then clearly m divides $2{\cdot}(a - b) = 2{\cdot}a - 2{\cdot}b$

   (d) If $a \equiv b \pmod{m}$, then $2{\cdot}a \equiv 2{\cdot}b \pmod{2{\cdot}m}$

   > **Solution:** `true` - if m divides $a - b$, then clearly $2{\cdot}m$ divides $2{\cdot}(a - b) = 2{\cdot}a - 2{\cdot}b$

   (e) If $a \equiv b \pmod{m}$, then $a \equiv b \pmod{2{\cdot}m}$

Solution: `false` - for example, considering $a = 1$, $b = 3$ and $m = 2$, then

- $1 \equiv 3 \pmod 2$ since 2 divides $1-3 = -2$;
- $1 \not\equiv 3 \pmod 4$ since 4 does not divide $1-3 = -2$.

(f) If $a \equiv b \pmod{2{\cdot}m}$, then $a \equiv b \pmod m$

Solution: `true` - if $2{\cdot}m$ divides $a - b$, then, since m divides $2{\cdot}m$, it follows that m divides $a - b$

(g) If $a \equiv b \pmod{m^2}$, then $a \equiv b \pmod m$

Solution: `true` - if m^2 divides $a - b$, then, since m divides m^2, it follows that m divides $a - b$

6. Use the Euclidean algorithm to find:

(a) $\gcd(44, 52)$;

Solution:

$$\begin{aligned} 52 &= 44{\cdot}1 + 8 \\ 44 &= 8{\cdot}5 + 4 \\ 8 &= 4{\cdot}2 + 0 \end{aligned}$$

Therefore $\gcd(44, 52) = 4$

(b) $\gcd(201, 302)$;

Solution:

$$\begin{aligned} 302 &= 201{\cdot}1 + 101 \\ 201 &= 101{\cdot}1 + 100 \\ 101 &= 100{\cdot}1 + 1 \\ 100 &= 1{\cdot}100 + 0 \end{aligned}$$

Therefore $\gcd(201, 302) = 1$

(c) $\gcd(184, 233)$.

Solution:

$$\begin{aligned} 233 &= 184{\cdot}1 + 49 \\ 184 &= 49{\cdot}3 + 37 \\ 49 &= 37{\cdot}1 + 12 \\ 37 &= 12{\cdot}3 + 1 \\ 12 &= 1{\cdot}12 + 0 \end{aligned}$$

Therefore $\gcd(184, 233) = 1$

7. Compute $A{+}B$ when the matrices A and B are given by:

$$A = \begin{pmatrix} 4 & -1 & 0 & 3 \\ 3 & 0 & 8 & 6 \\ 12 & 3 & -6 & 2 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & -5 & 4 & 1 \\ 2 & 0 & 12 & 3 \\ 9 & 6 & 7 & -5 \end{pmatrix}$$

Solution:

$$A{+}B = \begin{pmatrix} 4{+}0 & -1{+}(-5) & 0{+}4 & 3{+}1 \\ 3{+}2 & 0{+}0 & 8{+}12 & 6{+}3 \\ 12{+}9 & 3{+}6 & -6{+}7 & 2{+}-5 \end{pmatrix} = \begin{pmatrix} 4 & -6 & 4 & 4 \\ 5 & 0 & 20 & 9 \\ 21 & 9 & 1 & -3 \end{pmatrix}$$

8. Compute $A{\times}B$ when the matrices A and B are given by:

$$A = \begin{pmatrix} 4 & -1 & 0 & 3 \\ 3 & 0 & 8 & 6 \\ 12 & 3 & -6 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 8 & 4 & 13 & 6 & 0 \\ 0 & -5 & 4 & 7 & 3 \\ 2 & 0 & 12 & -4 & 1 \\ 9 & 6 & -7 & 0 & 5 \end{pmatrix}$$

Solution:

$$\begin{aligned} A{\times}B &= \begin{pmatrix} 32{+}0{+}0{+}27 & 16{+}5{+}0{+}18 & 52{-}4{+}0{-}21 & 24{-}7{+}0{+}0 & 0{-}3{+}0{+}15 \\ 24{+}0{+}16{+}54 & 12{-}0{+}0{+}36 & 39{+}0{+}96{-}42 & 18{+}0{-}32{+}0 & 0{+}0{+}8{+}30 \\ 96{+}0{-}12{+}0 & 48{-}15{+}0{+}0 & 156{+}12{-}72{+}0 & 72{+}21{+}24{+}0 & 0{+}9{-}6{+}0 \end{pmatrix} \\ &= \begin{pmatrix} 59 & 39 & 27 & 17 & 12 \\ 94 & 48 & 93 & -14 & 38 \\ 84 & 33 & 96 & 117 & 3 \end{pmatrix} \end{aligned}$$

9. (a) Suppose A and B are $m{\times}k$ matrices and C is a $k{\times}n$ matrix, show that:

$$(A + B){\times}C \quad = \quad A{\times}C + B{\times}C\,.$$

Solution: If $A = [a_{i,j}]$, $B = [b_{i,j}]$ and $C = [c_{i,j}]$, then by definition of matrix sum $A{+}B = [a_{i,j} + b_{i,j}]$ and by definition of matrix product:

$$\begin{aligned} (A+B){\times}C &= \left[\textstyle\sum_{r=1}^{k}(a_{i,r} + b_{i,r}){\cdot}c_{r,j}\right] & \\ &= \left[\textstyle\sum_{r=1}^{k}(a_{i,r}{\cdot}c_{r,j} + b_{i,r}{\cdot}c_{r,j})\right] & \text{rearranging} \\ &= \left[\textstyle\sum_{r=1}^{k}a_{i,r}{\cdot}c_{r,j} + \sum_{r=1}^{k}b_{i,r}{\cdot}c_{r,j}\right] & \text{rearranging} \\ &= \left[\textstyle\sum_{r=1}^{k}a_{i,r}{\cdot}c_{r,j}\right] + \left[\textstyle\sum_{r=1}^{k}b_{i,r}{\cdot}c_{r,j}\right] & \text{by definition of matrix sum} \\ &= A{\times}C + B{\times}C & \text{by definition of matrix product} \end{aligned}$$

(b) Suppose C is an $m\times k$ matrix and A and B are $k\times n$ matrices, show that:

$$C\times(A+B) \;=\; C\times A + C\times B\,.$$

Solution: If $A = [a_{i,j}]$, $B = [b_{i,j}]$ and $C = [c_{i,j}]$, then by definition of matrix sum $A+B = [a_{i,j} + b_{i,j}]$ and by definition of matrix product:

$$\begin{aligned}
C\times(A+B) &= \left[\textstyle\sum_{r=1}^{k} c_{i,r}\cdot(a_{r,j} + b_{r,j})\right] \\
&= \left[\textstyle\sum_{r=1}^{k} (c_{i,r}\cdot a_{r,j} + c_{i,r}\cdot b_{r,j})\right] && \text{rearranging} \\
&= \left[\textstyle\sum_{r=1}^{k} c_{i,r}\cdot a_{r,j} + \sum_{r=1}^{k} c_{i,r}\cdot b_{r,j}\right] && \text{rearranging} \\
&= \left[\textstyle\sum_{r=1}^{k} c_{i,r}\cdot a_{r,j}\right] + \left[\textstyle\sum_{r=1}^{k} c_{i,r}\cdot b_{r,j}\right] && \text{by definition of matrix sum} \\
&= C\times A + C\times B && \text{by definition of matrix product}
\end{aligned}$$

10. Let A and B be two $n\times n$ matrices, show that:

(a) $(A+B)^t = A^t + B^t$;

Solution: If $A = [a_{i,j}]$ and $B = [b_{i,j}]$, then by definition of matrix sum $A+B = [c_{i,j}] = [a_{i,j} + b_{i,j}]$ and hence, by definition of transpose:

$$\begin{aligned}
(A+B)^t &= [c_{j,i}] \\
&= [a_{j,i} + b_{j,i}] && \text{from above} \\
&= [a_{j,i}] + [b_{j,i}] && \text{by definition of matrix sum} \\
&= A^t + B^t && \text{by definition of matrix transpose}
\end{aligned}$$

(b) $(A\times B)^t = B^t\times A^t$.

Solution: If $A = [a_{i,j}]$ and $B = [b_{i,j}]$, then by definition of matrix product $A\times B = [c_{i,j}] = [\sum_{r=1}^{m} a_{i,r}\cdot b_{r,j}]$ and hence, by definition of matrix transpose:

$$\begin{aligned}
(A\times B)^t &= [c_{j,i}] \\
&= [\textstyle\sum_{r=1}^{m} a_{j,r}\cdot b_{r,i}] && \text{from above} \\
&= [\textstyle\sum_{r=1}^{m} b_{r,i}\cdot a_{j,r}] && \text{rearranging} \\
&= B^t\times A^t && \text{by definition of matrix product and transpose}
\end{aligned}$$

Difficult/challenging questions.

11. Show we can easily factor a number n when we know that it is the product of two primes p and q and we know the value of $(p-1)\cdot(q-1)$.

Solution: Factoring in this case reduces to finding the values of p and q when we know the value of their product, i.e. n and the value of $(p-1)\cdot(q-1)$. Now letting $(p-1)\cdot(q-1) = m$ we have:

$$m = (p-1)\cdot(q-1) = p\cdot q - p - q + 1$$

rearranging and using the fact that $n = p\cdot q$ ir follows that:

$$p + q = n + 1 - m$$

Now, again using the fact that $n = p\cdot q$, we have:

$$\begin{aligned} p + n/p = n + 1 - m \Rightarrow\ & p^2 + n = (n+1-m)\cdot p && \text{rearranging} \\ \Rightarrow\ & p^2 - (n+1-m)\cdot p + n = 0 && \text{rearranging again.} \end{aligned}$$

Similarly, we can show:

$$q^2 - (n+1-m)\cdot q + n = 0$$

and hence p and q are the two solutions of the quadratic equation:

$$x^2 - (n+1-m)\cdot x + n = 0$$

and since we know the values of n and m we can easily solve this using the formula:

$$x = \frac{-b \pm \sqrt{b^2 - 4a\cdot c}}{2}$$

with $a = 1$, $b = -(n+1-m)$ and $c = n$.

12. Let A be a $2{\times}2$ matrix where:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Under the assumption that $a\cdot d - b\cdot c \neq 0$ find the inverse of A.

Solution: Suppose the inverse of A is given by:

$$A^{-1} = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

then by definition of matrix multiplication we have:

$$A{\times}A^{-1} = \begin{pmatrix} a\cdot e + b\cdot g & a\cdot f + b\cdot h \\ c\cdot e + d\cdot g & c\cdot f + d\cdot h \end{pmatrix}$$

Now to be the inverse we require that the product equals the identity matrix and therefore:

$$\begin{aligned} a\cdot e + b\cdot g &= 1 \\ a\cdot f + b\cdot h &= 0 \\ c\cdot e + d\cdot g &= 0 \\ c\cdot f + d\cdot h &= 1 \end{aligned}$$

Solving these equations for e, f, g and h, under the assumption $a\cdot d - b\cdot c \neq 0$, we find that:

$$A^{-1} = \begin{pmatrix} \frac{d}{a\cdot d-b\cdot c} & \frac{-b}{a\cdot d-b\cdot c} \\ \frac{-c}{a\cdot d-b\cdot c} & \frac{a}{a\cdot d-b\cdot c} \end{pmatrix}$$