Euclidean Algorithm Solutions

Justin Stevens

Problem 1. (Mandelbrot) Compute $\gcd(2001, 25001)$.

Solution. Using the division algorithm, we see that

$$\begin{aligned} 25001 &= 2001 \cdot 12 + 989 \\ 2001 &= 989 \cdot 2 + 23 \\ 989 &= 23 \cdot 43. \end{aligned}$$

Hence, $\gcd(2001, 25001) = \boxed{23}$. ☐

Problem 2. (i) Find a pair of integers (m, n) satisfying $17m + 59n = 1$.

(ii) Solve the linear congruence $17x \equiv 3 \pmod{59}$.

Solution. (i) Using the division algorithm, we see that

$$\begin{aligned} 59 &= 17 \cdot 3 + 8 \\ 17 &= 8 \cdot 2 + 1. \end{aligned}$$

Hence, rewriting the equations, we see that

$$1 = 17 - 8 \cdot 2 = 17 - (59 - 17 \cdot 3) \cdot 2 = 17 \cdot 7 - 59 \cdot 2.$$

Therefore, the pair $(m, n) = \boxed{(7, -2)}$ suffice.

(ii) From above, we have $17 \cdot 7 \equiv 1 \pmod{59}$. Multiplying this congruence by 3 we arrive at $17 \cdot 21 \equiv 3 \pmod{59}$. Hence, $x \equiv \boxed{21 \pmod{59}}$.

☐

Problem 3. (PuMaC) Compute $\gcd(2^{30^{10}} - 2, 2^{30^{45}} - 2)$. Leave your answer in exponential form.

Solution. Recall that $\gcd(n^a - 1, n^b - 1) = n^{\gcd(a,b)} - 1$. Factoring out 2 and applying this theorem twice gives

$$\begin{aligned} \gcd(2^{30^{10}} - 2, 2^{30^{45}} - 2) &= 2\gcd(2^{30^{10}-1} - 1, 2^{30^{45}-1} - 1) \\ &= 2\left(2^{\gcd(30^{10}-1, 30^{45}-1)} - 1\right) \\ &= 2\left(2^{30^{\gcd(10,45)}-1} - 1\right) \\ &= 2\left(2^{30^5-1} - 1\right) \\ &= \boxed{2^{30^5} - 2}. \end{aligned}$$

☐

Problem 4. Prove that if $\gcd(a,b)=d$, then $\gcd(\frac{a}{d},\frac{b}{d})=1$. *Hint:* Use Bezout's theorem.

Solution. Since $d \mid a$ and $d \mid b$, there exist integers a' and b' such that $a=da'$ and $b=db'$.
From Bezout's theorem, there exists integers x and y such that

$$ax+by=d \implies da'x+db'y=d \implies a'x+b'y=1.$$

From Bezout's again, $\gcd(a',b')=1$. Since $a'=\frac{a}{d}$ and $b'=\frac{b}{d}$, we are finished. □

Problem 5. (i) Prove that if a and b are relatively prime, then $\gcd(ab,a+b)=1$.

Hint: Use Euclid's Lemma and proof by contradiction.

(ii) Prove that $\gcd(a+b,a^2-ab+b^2)=\begin{cases}1 \text{ if } 3\nmid a+b\\ 3 \text{ if } 3\mid a+b.\end{cases}$

Solution. (i) Assume for the sake of contradiction that they are not relatively prime. This implies that there exists a prime p such that $p\mid ab$ and $p\mid a+b$.

From Euclid's lemma, $p\mid ab \implies p\mid a$ or $p\mid b$. However, if $p\mid a$ for instance, then from $p\mid a+b$, we must also have $p\mid b$. This contradicts the fact that a and b are relatively prime. Therefore, it is impossible to find such a prime p, and $\gcd(ab,a+b)=1$.

(ii) Using the Euclidean algorithm, we see that since $(a+b)^2=a^2+2ab+b^2$, we have

$$\gcd(a+b,a^2-ab+b^2)=\gcd(a+b,a^2+2ab+b^2-\big(a^2-ab+b^2\big))=\gcd(a+b,3ab).$$

From above, we know that if $\gcd(a,b)=1$, then $\gcd(a+b,ab)=1$. Therefore, if $3\mid a+b$, then $\gcd(a+b,a^2-ab+b^2)=3$. Otherwise, if $3\nmid a+b$, then $\gcd(a+b,a^2-ab+b^2)=1$. □

Problem 6. The Fibonacci numbers are defined by $F_1=1,F_2=1$, and $F_{n+2}=F_{n+1}+F_n$.

(i) Prove that any two consecutive Fibonacci numbers are relatively prime using induction.

(ii) Prove that $F_m\mid F_{mq}$ for all natural q using the identity $F_{a+b}=F_{a+1}F_b+F_aF_{b-1}$.

($\star$) Prove that $\gcd(F_n,F_m)=F_{\gcd(n,m)}$. *Hint:* Write $n=mq+r$.

Solution. (i) We use the method of induction to prove the statement $\gcd(F_{n+1},F_n)=1$. If $n=1$, then this is equivalent to $\gcd(F_2,F_1)=\gcd(1,1)=1$. Now, we assume the statement is true for $n=k$. For $n=k+1$ we see that

$$\gcd(F_{k+2},F_{k+1})=\gcd(F_{k+2}-F_{k+1},F_{k+1})=\gcd(F_k,F_{k+1})=1$$

using the inductive hypothesis and the definition of Fibonacci numbers.

(ii) We once again use the method of induction. For $q = 1$, we have $F_m \mid F_m$. For $q = 2$, we see that $F_{2m} = F_{m+1}F_m + F_mF_{m-1}$ using the identity, therefore, $F_m \mid F_{2m}$.

Now, we assume the statement is true for an arbitrary q and show it holds for $q+1$. We see that from the identity,

$$F_{mq+m} = F_{mq+1}F_m + F_{mq}F_{m-1}.$$

From the inductive hypothesis, $F_m \mid F_{mq}$, therefore, we see that $F_m \mid F_{mq+m}$. Hence, we have proven the statement for $q+1$ and our induction is complete.

(iii) Write $n = mq + r$ using the division algorithm. Using the Fibonacci identity,

$$F_n = F_{mq+r} = F_{mq+1}F_r + F_{mq}F_{r_1}.$$

Now, since $F_m \mid F_{mq}$, we can subtract multiples of F_m using the Euclidean algorithm:

$$\gcd(F_n, F_m) = \gcd(F_{mq+1}F_r + F_{mq}F_{r-1}, F_m) = \gcd(F_{mq+1}F_r, F_m).$$

Finally, we have $\gcd(F_{mq+1}, F_m)$ since $F_m \mid F_{mq}$ and consecutive Fibonacci numbers are relatively prime. Therefore,

$$\gcd(F_n, F_m) = \gcd(F_r, F_m).$$

The conclusion is hence that $\gcd(F_n, F_m) = \gcd(F_m, F_r)$ as in the Euclidean algorithm. This implies that $\gcd(F_n, F_m) = F_{\gcd(m,n)}$. For instance,

$$\gcd(F_{182}, F_{65}) = \gcd(F_{65}, F_{52}) = \gcd(F_{52}, F_{13}) = F_{13}$$

and $\gcd(182, 65) = 13$.

$\square$