MA2316: solutions to (part B of) study week challenge

1. Note that
$$\frac{233+387i}{103+363i}=\frac{320}{277}-\frac{87}{277}i\approx 1,$$
so the first round of the Euclidean algorithm tells us that
$$\gcd(103+363i,233+387i)=\gcd(103+363i,233+387i-103-363i)=\gcd(103+363i,130+24i).$$
Furthermore,
$$\frac{103+363i}{130+24i}=\frac{43}{34}+\frac{87}{34}\approx 1+3i,$$
so the second round of the Euclidean algorithm tells us that
$$\gcd(103+363i,130+24i)=\gcd(130+24i,103+363i-(130+24i)(1+3i))=\gcd(130+24i,45-51i).$$
One further step gives us
$$\frac{130+24i}{45-51i}=1+\frac{5}{3}i\approx 1+2i,$$
so
$$\gcd(130+24i,45-51i)=\gcd(45-51i,130+24i-(45-51i)(1+2i))=\gcd(45-51i,-17-15i).$$
Since $45-51i=(-17-15i)(-3i)$, we conclude that
$$\gcd(103+363i,233+387i)=-17-15i$$
(or one of the Gaussian integers differing from that by an invertible factor).

2. Recall that a number is congruent to the sum of its decimal digits modulo 9, so
$$n^{23}\equiv 3+7+9+2+6+4+3+4+8+8+0+0+6+8+2+9+8+9+3+2+2+1+3+9+$$
$$+9+4+4+0+9+9+2+2+1+4+6+0+4+5+4+4+3+1+1\equiv 8\equiv -1 \pmod 9.$$
Also, we trivially have $n^{23}\equiv 1 \pmod{10}$, since the last decimal digit of n^{23} is 1.

Note that if n is not coprime to 9, then n^{23} is not coprime to 9, which we know is not the case, as $n^{23}\equiv -1 \pmod 9$. Also, if n is not coprime to 10, then n^{23} is not coprime to 10, which we know is not the case, as $n^{23}\equiv 1 \pmod{10}$.

We have $\varphi(10)=\varphi(2)\varphi(5)=4$, so for each x coprime to 10 we have $x^4\equiv 1 \pmod{10}$ by Euler's theorem, and hence $x^{24}=(x^4)^6\equiv 1 \pmod{10}$. Therefore, $n^{23}\equiv n^{-1} \pmod{10}$, and we conclude that $n^{-1}\equiv 1 \pmod{10}$, which in turn implies $n\equiv 1 \pmod{10}$.

Also, $\varphi(9)=9-3=6$, so for each x coprime to 3 we have $x^6\equiv 1 \pmod 9$, and hence $x^{24}=(x^6)^4\equiv 1 \pmod 9$. Therefore, $-1\equiv n^{23}\equiv n^{-1} \pmod 9$, and $n\equiv -1 \pmod 9$. We conclude that
$$\begin{cases} n\equiv 1 \pmod{10},\\ n\equiv -1 \pmod 9.\end{cases}$$
Solving this system of congruences, we get $n\equiv 71 \pmod{90}$. If $n>71$, then $n\geqslant 161>100$, so n^{23} has at least 46 digits. We conclude that $n=71$.

3. Note that $507=3\cdot 13^2$, so in order to solve this congruence, we should solve it modulo 3, solve it modulo 13, lift the solution modulo 13 in $\mathbb{Z}/13^2\mathbb{Z}$, and merge the result with the modulo 3 answer using the Chinese Remainder Theorem.

First of all, by inspection we see that $x=1$ is the only solution modulo 3. As for modulo 13, we note that $3^2+3+1=13$, so 3 is a solution, and since the sum of roots of a quadratic equation is the negative of the coefficient at x, we conclude that $-1-3 \equiv 9 \pmod{13}$ is also a solution. Let us now lift these modulo 13^2. Note that $(x^2+x+1)' = 2x+1$, so it does not vanish for $x = 3$ or for $x = 9$, and hence Hensel's lemma guarantees that the lifts of roots modulo 13^2 exist and are unique. We have

$$(3+13k)^2 + (3+13k) + 1 \equiv 9 + 2 \cdot 3 \cdot 13k + 3 + 13k + 1 \equiv 13(1+7k) \pmod{13^2},$$

so $k = 11$ works, and 146 is a root modulo 13^2. Also,

$$(9+13k)^2 + (9+13k) + 1 \equiv 81 + 2 \cdot 9 \cdot 13k + 9 + 13k + 1 \equiv 13(7+6k) \pmod{13^2},$$

so $k = 1$ works, and 22 is a root modulo 13^2. Finally, we need to combine it with $x \equiv 1 \pmod 3$. Since $13^2 \cdot 1 + 3 \cdot (-56) = 1$, we conclude that $1 \cdot 13^2 \cdot 1 + 22 \cdot 3 \cdot (-56) = -3527 \equiv 22 \pmod{507}$ and $1 \cdot 13^2 \cdot 1 + 146 \cdot 3 \cdot (-56) = -24359 \equiv 484 \pmod{507}$ are the only solutions.

Remark: one can note that we have $9 = 3^2$ for solutions modulo 13 and $484 = 22^2$ for solutions modulo 507, even further, we have $146 \equiv 22^2 \pmod{13^2}$. It is not completely coincidental, since $x^2 + x + 1 = 0$ means that $x^3 = 1$, and if a is a root of this equation, then a^2 is clearly also a root.

4. Note that modulo 2 this solution has a solution $x = 1$, so in what follows we assume p odd. First of all, $x^4 = (x^2)^2$, so if the congruence $x^4 \equiv -1 \pmod p$ has solutions, then $x^2 \equiv -1 \pmod p$ also has solutions. We know that $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, so we conclude that $p \equiv 1 \pmod 4$, $p = 4m + 1$. Now, for such x let a be such that $a^2 \equiv -1 \pmod p$, so the congruence $x^4 \equiv -1 \pmod p$ becomes $x^4 \equiv a^2 \pmod p$, that is $x^2 \equiv a \pmod p$ or $x^2 \equiv -a \equiv a^3 \pmod p$. Thus, our equation has solutions if $\left(\frac{a}{p}\right) = 1$. We recall that $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$, so

$$\left(\frac{a}{p}\right) \equiv a^{2m} \equiv (a^2)^m \equiv (-1)^m \pmod p,$$

and we conclude that for odd p the congruence $x^4 \equiv -1 \pmod p$ has solutions if and only $p \equiv 1 \pmod 8$.