MATH 135 Winter 2020: Final Assignment

Q01. Let p, q, r be distinct primes. Determine $\gcd(p^{10}q^{20}r^{30}, (p^2qr^2)^{10})$ in terms of p, q, r.

Solution. Since p, q, and r are distinct, the quantities $p^{10}q^{20}r^{30}$ and $(p^2qr^2)^{10} = p^{20}q^{10}r^{20}$ are in their UPF form. Then, apply GCD PF: $\gcd(p^{10}q^{20}r^{30}, p^{20}q^{10}r^{20}) = p^{10}q^{10}r^{20}$. $\square$

Q02. Given that $[x_0] = [6]$ is a solution to $[12][x] = [8]$ in $\mathbb{Z}_{64}$, write down the complete solution. Express your answer(s) in the form $[a]$, where a is an integer and $0 \le a < 64$.

Solution. By the Modular Arithmetic Theorem, there are $\gcd(12, 64) = 4$ solutions, which are of the form $[6 + \frac{64}{4}k]$ for $0 \le k < 4$. That is, $[x]$ is one of $[6]$, $[22]$, $[38]$, or $[54]$. $\square$

Q03. Determine the units digit (i.e., the ones digit) of 7^{202}.

Solution. We must evaluate $7^{202} \pmod{10}$. Since $7^2 \equiv 49 \equiv -1 \pmod{10}$, it follows that $7^{202} \equiv (7^2)^{101} \equiv (-1)^{101} \equiv -1 \equiv 9 \pmod{10}$.

Therefore, the last digit is 9. $\square$

Q04. Write $(2 - 2i)^6$ in standard form.

Solution. Notice that $2 - 2i = 2(1 - i) = 2\sqrt{2}\operatorname{cis}(-\frac{\pi}{4})$. Then, we distribute and apply DMT: $(2\sqrt{2}\operatorname{cis}(-\frac{\pi}{4}))^6 = (2\sqrt{2})^6 \operatorname{cis}(-\frac{3\pi}{2}) = 512\operatorname{cis}(\frac{\pi}{2})$.

It follows that in standard form, $(2 - 2i)^6 = 0 + 512i$. $\square$

Q05. Find all $z \in \mathbb{C}$ that satisfy the equation $z^6 = 32z$. You may express your solution(s) in polar form.

Solution. We have $z^6 = 32z \iff z^5 = 32$. In polar form, $32 = 32\operatorname{cis} 0$. By CNRT, we have the fifth roots of 32 are

$$2\operatorname{cis} 0, 2\operatorname{cis}\frac{2\pi}{5}, 2\operatorname{cis}\frac{4\pi}{5}, 2\operatorname{cis}\frac{6\pi}{5}, 2\operatorname{cis}\frac{8\pi}{5}$$ $\square$

Q06. Determine all integer solutions (x, y) to the linear Diophantine equation $21x + 15y = 72$ such that $x \ge 0$ and $y \ge 0$.

Solution. We apply the EEA:

x	y	q	r
1	0	21	
0	1	15	
1	-1	6	1
-2	3	3	2

We can stop since $3 \mid 6$ and conclude $\gcd(21, 15) = 3$. Now, $21(-2) + 15(3) = 3$ and multiplying through by 24, we have $21(-48) + 15(72) = 72$.

It follows by the LDET that the set of all solutions is given by

$$\{(-48 + 5n, 72 - 7n) : n \in \mathbb{Z}\}$$

If both x and y are positive, then $-48 + 5n > 0 \iff n > \frac{48}{5} \iff n \ge 10$ and $72 - 7n > 0 \iff n < \frac{72}{7} \iff n \le 10$.

The only such value is $n = 10$ so the only such solution is $x = 2$ and $y = 2$. $\square$

Q07. Let $z, w \in \mathbb{C}$ such that $|z| = |w| = 2$ and $z\overline{w} = 1 + i$. Determine $|z - w|^2$.

Solution. Let $z = a + bi$ and $w = c + di$ be complex numbers with modulus 2 where $z\overline{w} = 1 + i$. Then, by definition, $a^2 + b^2 = c^2 + d^2 = \sqrt{2}$ and $(a + bi)(c - di) = 1 + i$. From the second equation, we have $(ac + bd) + (bc - ad)i = 1 + i$. Equating real parts, $ac + bd = 1$. Now,

$$
\begin{aligned}
|z - w|^2 &= |(a - c) + (b - d)|^2 \\
&= (a - c)^2 + (b - d)^2 \\
&= a^2 - 2ac + c^2 + b^2 - 2bc + d^2 \\
&= (a^2 + b^2) + (c^2 + d^2) - 2(ac + bd) \\
&= \sqrt{2} + \sqrt{2} - 2(1) \\
&= 2\sqrt{2} - 2
\end{aligned}
$$

□

Q08. You are an eavesdropper who has intercepted the ciphertext $C = 9$ sent using RSA. You have obtained the public key $(29, 91)$ and have managed to factor $n = 91$ as $7 \cdot 13$.

Determine the original message M.

Solution. Let $p = 7$ and $q = 13$, so our secret modulus is $6 \cdot 12 = 72$. We determine the privkey d knowing that $ed \equiv 29d \equiv 1 \pmod{72}$. Solving by SMT, $29d \equiv 5d \equiv 1 \pmod{8}$ and $29d \equiv 2d \equiv 1 \pmod{9}$.

From the first congruence, by inspection $d = 5$ works, so LCT gives $d \equiv 5 \pmod{8}$ as the full solution set. So, $d = 8k + 5$ for some integer k. Substituting, $2(8k + 5) \equiv 16k + 10 \equiv 7k + 10 \equiv 1 \pmod{9}$. Then, $7k \equiv 0 \pmod{9}$ and by inspection $k \equiv 0 \pmod{9}$. Finally, $d = 8(9n) + 5 = 72n + 5$ with integer n, or, $d \equiv 5 \pmod{72}$. Indeed, $0 < d < 72$.

Therefore, $d = 5$.

We decode the message knowing $M \equiv C^d \equiv 9^5 \pmod{91}$. Repeatedly squaring, we have $9^2 \equiv 81 \equiv -10 \pmod{91}$, and $9^4 \equiv 100 \equiv 9 \pmod{91}$.

Therefore, $M \equiv 9^{4+1} \equiv (9)(9) \equiv 9^2 \equiv -10 \equiv 81 \pmod{91}$, so $M = 81$. □

Q09. It is known that $3i$ is a root of the polynomial $f(x) = 2x^5 - 5x^4 + 18x^3 - 44x^2 + 9$.

(a) Write $f(x)$ as a product of irreducible polynomials in $\mathbb{C}[x]$.

Solution. The CPN gives that $f(x)$ has 5 complex roots, so we must find 5 complex linear factors. By the CJRT, $-3i$ is also a root of $f(x)$. Then, by the Factor Theorem, $(x - 3i)(x + 3i) = (x^2 + 9) \mid f(x)$. By long division:

$$
\begin{array}{r r}
 & 2x^3 \quad - 5x^2 + 1 \\ \cline{2-2}
x^2 + 9) & 2x^5 - 5x^4 + 18x^3 - 44x^2 + 9 \\
 & - 2x^5 \qquad\quad - 18x^3 \qquad\qquad\quad \\ \cline{2-2}
 & - 5x^4 \qquad\quad - 44x^2 \qquad \\
 & 5x^4 \qquad\quad + 45x^2 \qquad \\ \cline{2-2}
 & x^2 + 9 \\
 & - x^2 - 9 \\ \cline{2-2}
 & 0
\end{array}
$$

Inspecting candidates from the Rational Roots Theorem, we find $f(\frac{1}{2}) = 0$.

We divide by $(2x-1)$:

$$
\begin{array}{r|l}
 & x^2 - 2x - 1 \\
\hline
2x-1 & 2x^3 - 5x^2 \qquad + 1 \\
 & -2x^3 + x^2 \\
\hline
 & -4x^2 \\
 & 4x^2 - 2x \\
\hline
 & -2x + 1 \\
 & 2x - 1 \\
\hline
 & 0
\end{array}
$$

Finally, the quadratic formula gives $f(1 \pm \sqrt{2}) = 0$. From these five roots, we multiply the of irreducible first degree factors to get

$$f(x) = (x - 3i)(x + 3i)(2x - 1)(x - 1 + \sqrt{2})(x - 1 - \sqrt{2}) \qquad \square$$

(b) Write $f(x)$ as a product of irreducible polynomials in $\mathbb{R}[x]$.

Solution. Since $\mathbb{R}[x] \subsetneq \mathbb{C}[x]$, we can consider the factorization from (a). From (a), the only factors not in $\mathbb{R}[x]$ are $(x - 3i)$ and $(x + 3i)$. Then,

$$f(x) = (x^2 + 9)(2x - 1)(x - 1 + \sqrt{2})(x - 1 - \sqrt{2}) \qquad \square$$

(c) Write $f(x)$ as a product of irreducible polynomials in $\mathbb{Q}[x]$.

Solution. Again, $\mathbb{Q}[x] \subsetneq \mathbb{R}[x]$. The only factors in (b) not in $\mathbb{Q}[x]$ are $(x - 1 \pm \sqrt{2})$. Then,

$$f(x) = (x^2 + 9)(2x - 1)(x^2 - 2x - 1) \qquad \square$$

Q10. True or False. Indicate whether each statement is true or false.

(a) For all $f(x) \in \mathbb{R}[x]$, if $f(x)$ has no real roots, then $f(x)$ is irreducible in $\mathbb{R}[x]$.

True $\boxed{\text{False}}$ *Counterexample: take* $f(x) = x^4 + 2x^2 + 1 = (x^2 + 1)(x^2 + 1)$

(b) $\{x \in \mathbb{Z} : \gcd(x, 20) = 1\} = \{y \in \mathbb{Z} : \gcd(2y, 40) = 2\}$.

$\boxed{\text{True}}$ False *Use BL to simplify RHS into LHS*

(c) There are infinitely many integers x satisfying the simultaneous congruence

$$
\begin{aligned}
2x &\equiv 4 \pmod{8} \\
x + 1 &\equiv 5 \pmod{7}
\end{aligned}
$$

$\boxed{\text{True}}$ False *Simplifies to* $x \equiv 18 \pmod{28}$

(d) For every $a \in \mathbb{Z}$, the LDE $(2a + 1)x + ay = 1$ has a solution.

$\boxed{\text{True}}$ False *Since* $\gcd(2a + 1, a) = \gcd(a, 1) = 1$

(e) In $\mathbb{Z}_{48}$, the equation $[9][x] = [4]$ has exactly 3 solutions.

True $\boxed{\text{False}}$ *There are none.*

(f) For all $d \in \mathbb{Z}$, if $d \mid 10$ and $d \mid 15$ and $d \mid 10s + 15t$ for some $s, t \in \mathbb{Z}$, then $d = 5$.

True $\boxed{\text{False}}$ *No special d by DIC*

(g) For all polynomials $f(x)$ with integer coefficients, if $f(\frac{\sqrt{2}}{1+i}) = 0$, then $f(\frac{1+i}{\sqrt{2}}) = 0$.

$\boxed{\text{True}}$ False *Since they are* $\frac{\sqrt{2}}{2} \pm \frac{\sqrt{2}}{2}i$

Q11. Prove that there does not exist an integer x such that $x^2 \equiv 5 \pmod 6$.

Proof. We exhaust the values of $x \pmod 6$:

$x \pmod 6$	0	1	2	3	4	5
$x^2 \pmod 6$	0	1	4	3	4	1

Notice that no x satisfies $x^2 \equiv 5 \pmod 6$. □

Q12. Let p be an odd prime, and let a be an odd integer such that $p \nmid a$. Prove that

$$a^{p-1} \equiv 1 \pmod{2p}.$$

Proof. Let p be an odd prime, that is, $p \neq 2$, and a be an odd integer not a multiple of p. By FℓT, $a^{p-1} \equiv 1 \pmod p$. Since a is odd, $a \equiv 1 \pmod 2$ and $a^{p-1} \equiv 1 \pmod 2$ by CP. Then, by SMT, $a^{p-1} \equiv 1 \pmod{2p}$. □

Q13. Prove that for all $a, b, c \in \mathbb{Z}$, $c \mid \gcd(a, c) \cdot \gcd(b, c)$ if and only if $c \mid ab$.

Proof. Let a, b, and c be integers, and say $\gcd(a, c) = g$ and $\gcd(b, c) = h$. Then, by Bézout's Lemma, we can write $g = as + ct$ and $h = bu + cv$ for some integers s, t, u, v. Expanding, $gh = (as+ct)(bu+cv) = asbu+ascv+ctbu+c^2tv = ab(su)+c(asv+tbu+ctv)$.

($\Rightarrow$) Suppose that $c \mid gh$. By definition, $g \mid a$ and $h \mid b$. Then, $gn = a$ and $hm = b$ for some integers n and m. It follows that $gh(nm) = ab$ so $gh \mid ab$. Finally, by TD, $c \mid ab$.

($\Leftarrow$) Suppose that $c \mid ab$. Then, since $c \mid ab$ and $c \mid c$, by DIC as su and $asv + tbu + ctv$ are integers, $c \mid gh$, finishing the proof. □

Q14. Let $\theta \in \mathbb{R}$ be such that $2 \sin\theta \cos\theta = \frac{1}{\sqrt{2}}$. Prove that $\sin\theta + \cos\theta$ is irrational.

Proof. Let θ be a real number and $2 \sin\theta \cos\theta = \sin 2\theta = \frac{1}{\sqrt{2}}$. Then, WLOG, we restrict $0 \leq \theta < 2\pi$, so that $2\theta = \frac{\pi}{4}$ and $\theta = \frac{\pi}{8}$.

Now, recall the half-angle formulae for sine and cosine. We have

$$\sin\theta = \sin\left(\frac{\pi/4}{2}\right) = \sqrt{\frac{1 - \cos(\pi/4)}{2}} = \frac{\sqrt{2 - \sqrt{2}}}{2}$$

and

$$\cos\theta = \cos\left(\frac{\pi/4}{2}\right) = \sqrt{\frac{1 + \cos(\pi/4)}{2}} = \frac{\sqrt{2 + \sqrt{2}}}{2}$$

Then, $\sin\theta + \cos\theta = \frac{\sqrt{2-\sqrt{2}}+\sqrt{2+\sqrt{2}}}{2}$. Let $a = \sin\theta + \cos\theta$, so that

$$\begin{aligned} 2a &= \sqrt{2 - \sqrt{2}} + \sqrt{2 + \sqrt{2}} \\ 4a^2 &= 4 + 2\sqrt{2} \\ (a^2 - 1)^2 &= 2 \\ 0 &= a^4 - 2a^2 - 1 \end{aligned}$$

Let $f(x) = x^4 - 2x^2 - 1$ so that $f(a) = 0$ and a is a root of f. Then, the Rational Roots Theorem states that candidates for rational roots of f are ± 1. However, $f(1) = -2$ and $f(-1) = -2$. Therefore, there are no rational roots of f, so a is irrational. □