MATH 1025: Introduction to Cryptography

Final Review

Solutions

Problem 1. Let n be a positive odd integer.

(a) Prove that there is a 1-to-1 correspondence between the divisors of n which are $< \sqrt{n}$ and those that are $> \sqrt{n}$. (This part does not require n to be odd.)

Solution: let $a < \sqrt{n}$ be a divisor of n, then there is a number $b \in \mathbb{Z}_{>0}$, s.t. $ab = n$. Moreover, we must have $b > \sqrt{n}$, since otherwise $ab < (\sqrt{n})^2 = n$. Clearly, a determines b uniquely, as $b = \dfrac{n}{a}$.

(b) Prove that there is a 1-to-1 correspondence between all of the divisors of n which are $\geq \sqrt{n}$ and all the ways of writing n as a difference $s^2 - t^2$ of two squares of nonnegative integers. (For instance, 15 has two divisors 5 and 15 that are $\geq \sqrt{15}$, and $15 = 4^2 - 1 = 8^2 - 7^2$.

Solution: let $n = ab$ with $b \geq \sqrt{n}$, then one would like to find s and t, s.t. $n = ab = s^2 - t^2$:

$$\begin{cases} s - t = a \\ s + t = b, \end{cases}$$

giving $s = \dfrac{1}{2}(a+b)$ and $t = \dfrac{1}{2}(b-a)$, furthermore, both s and t are integers, since n is odd (implying a and b are odd as well). The correspondence between the pairs (a, b) and (s, t) is clearly bijective.

Problem 2. Prove that $n^5 - n$ is always divisible by 30.

Solution: we have $n^5 - n = n(n^4 - 1) = n(n^2+1)(n^2-1) = (n-1)n(n+1)(n^2+1)$, while $30 = 2 \cdot 3 \cdot 5$. Notice, that $n-1, n$ and $n+1$ are three consecutive integers, hence, their product is divisible by $2 \cdot 3 = 6$. It remains to show that the number $(n-1)n(n+1)(n^2+1)$ is divisible by 5. If $n \equiv 0, 1$ or $4 \pmod 5$, then one of the numbers $n-1, n$ or $n+1$ is divisible by 5. In case $n \equiv 2$ or $3 \pmod 5$, we get $2^2 + 1 \equiv 3^2 + 1 \equiv 0 \pmod 5$. The result follows.

Problem 3. Suppose that in tiling a floor that is 8×9 ft^2, you bought 72 tiles at a price you cannot remember. Your receipt gives the total cost as some amount under \$100, but the first and last digits are illegible. It reads '\$?0.6?'. How much did the tiles cost?

Solution: the number $n = a0.6b$ (here $0 \leq a \leq 9$ and $0 \leq b \leq 9$ stand for the missing digits) representing the price must be divisible by $72 = 8 \cdot 9$. Therefore

$$\begin{cases} a + 0 + 6 + b \equiv 0 \pmod 9 \\ 6b \equiv 0 \pmod 8. \end{cases}$$

It follows that $b = 4$, $a = 8$ and the price was \$80.64.

Problem 4. Let p be an odd prime. Prove that -3 is a quadratic residue in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 3$.

Solution: by definition of the Legendre symbol, -3 is a quadratic residue in $\mathbb{F}_p$ if and only if $\left(\frac{-3}{p}\right) = 1$. Using the properties of the Legendre symbol, we compute

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)(3-1)}{4}}\left(\frac{-1}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

The assertion follows.

Problem 5. Show that if p and $2p-1$ are both prime, and $n = p(2p-1)$, then n is a pseudoprime ($\gcd(b, n) = 1$ and $b^{n-1} \equiv 1 \pmod{n}$) for 50% of the possible bases b, namely for all b which are quadratic residues modulo $2p-1$.

Solution: $b^{n-1} \equiv b^{p(2p-1)-1} \equiv b^{(p-1)(2p+1)}$. Next, the Legendre symbol $\left(\frac{b}{2p-1}\right) = b^{\frac{2p-2}{2}} = b^{p-1} \pmod{2p-1}$ (Euler's property). On the other hand, $b^{p-1} \pmod{p}$ due to FLT. Hence, $\left(\frac{b}{2p-1}\right) = b^{p-1} \equiv 1 \pmod{2p-1}$ gives $b^{n-1} \equiv b^{(p-1)(2p+1)} \equiv 1 \pmod{n}$, while $\left(\frac{b}{2p-1}\right) = b^{p-1} \equiv -1 \pmod{2p-1}$ gives $b^{n-1} \equiv b^{(p-1)(2p+1)} \equiv -1 \pmod{n}$.

Problem 6. Compute the Legendre symbol $\left(\frac{3}{2729}\right)$ (the number 2729 is prime).

Solution: using law of quadratic reciprocity, we get $\left(\frac{3}{2729}\right) = (-1)^{1364} \cdot \left(\frac{2729}{3}\right) = \left(\frac{2}{3}\right) = -1$.

Problem 7. Let P be a point on a smooth elliptic curve over $\mathbb{R}$. Suppose that P is not the point at infinity.

(a) Give a geometric condition that is equivalent to P being a point of order 2.

Solution: the tangent line to E at P is vertical, hence these are the points of intersection of the graph of E with the x-axis (the graph of E is symmetric w.r.t. the x-axis and, as $-P$ is the reflection of P w.r.t. the x-axis, $P = -P$ only for P on the x-axis).

(b) Give a geometric condition (justify your answer) that is equivalent to P being a point of order 3.

Solution: such a point P satisfies $P \oplus P \oplus P = \mathcal{O}$ or $P \oplus P = -P$, which implies that the third point of intersection of the tangent line to E at P with the graph of E is P. Let $F_\ell(x)$ be the restriction of the defining polynomial of E to the tangent line to E at P. Then $F_\ell(x)$ vanishes at P with multiplicity 3, meaning that $F_\ell(x(P)) = F'_\ell(x(P)) = F''_\ell(x(P)) = 0$ (here $x(P)$ is the x-coordinate of P), thus P is an inflection point.

Problem 8. Let E be a smooth elliptic curve over $\mathbb{R}$.

(a) How many points (elements) of order 2 can $G(E)$ have? (justify your answer)

Solution: the cubic polynomial in the defining equation of E has either one or three real zeros and those are precisely the elements of order 2.

(b) Find the equation $\psi(x)$ that the x-coordinate of a point (element) satisfies if and only if it has order 3?[1] (justify your answer)

Solution: using implicit differentiation, we find $2y\dfrac{dy}{dx} = 3x^2 + a$, thus, $\dfrac{dy}{dx} = \dfrac{3x^2+a}{2y}$. Differentiating implicitly one more time gives

$$\frac{d^2y}{dx^2} = \frac{d\left(\dfrac{3x^2+a}{2y}\right)}{dx} = \frac{6x\cdot 2y - 2\dfrac{dy}{dx}(3x^2+a)}{4y^2} = \frac{12xy^2 - (3x^2+a)^2}{4y^3} = \frac{12x(x^3+ax+b) - (3x^2+a)^2}{4y^3},$$

so $\psi(x) = 12x(x^3+ax+b) - (3x^2+a)^2 = 3x^4 + 6ax^2 + 12bx - a^2$.

(c) Let's pick a concrete example with $b = 0, a = 1$, i.e. the defining equation of E is $y^2 = x^3 + x$. Find the inflection points (give both coordinates).

Solution: we have $\psi(x) = 3x^4 + 6x^2 - 1$ and using the substitution $t = x^2 \geq 0$, get the quadratic equation $\psi(t) = 3t^2 + 6t - 1$, which has the zeros $t_{1,2} = \dfrac{-6 \pm 4\sqrt{3}}{6}$. Notice that $t_2 = \dfrac{-6-4\sqrt{3}}{6}$ is less than 0, while $t_1 = \dfrac{-6+4\sqrt{3}}{6} = \dfrac{-3+2\sqrt{3}}{3}$ is greater. Notice that the domain of E is $x \geq 0$, hence, the only possible value of the x- coordinate is $\sqrt{\dfrac{-3+2\sqrt{3}}{3}}$. The inflection points are

$$P_1 = \left(\sqrt{\frac{-3+2\sqrt{3}}{3}}, \frac{2\sqrt{-3+2\sqrt{3}}}{3}\right)$$
$$P_2 = \left(\sqrt{\frac{-3+2\sqrt{3}}{3}}, -\frac{2\sqrt{-3+2\sqrt{3}}}{3}\right).$$

[1]**Hint:** hopefully, you found out that the answer in $6(b)$ is 'inflection points'. That means a point $P = (P_x, P_y)$ has order 3 iff $y''(P) = \dfrac{d^2y}{dx^2} = 0$. Find the second derivative using implicit differentiation of $y^2 = x^3 + ax + b$, the defining equation of E, twice. Then use the defining equation of E again to get rid of the y terms.