Spring 2021

MATH 1025: Introduction to Cryptography

Final Review

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.)

(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 $15 = 4^2 - 1 = 8^2 - 7^2$.

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

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?

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

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 $2p-1$.

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

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.

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

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)

(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)

(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)

---

[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.