CS 235: Algebraic Algorithms, Spring 2021

Homework 3

(Solutions for selected problems)

Problem 1. Exercise 26: Find all elements of $\mathbb{Z}_{19}^*$ of multiplicative order of 18.

Solution. Notice that 2 is a primitive root modulo 19 which means that $2^{18} \equiv 1 \pmod{19}$. Obviously, $2 \in \mathbb{Z}_{19}^*$ which is the first element that we are looking for.

(If the above fact was not obvious to you, then another way to do it is checking each 2^i for $i = 1, 2, 3, 6, 9, 18$ and you can verify that only 2^{18} is congruence to 1 mod 19. The reason is by Theorem 2.13, the multiplicative order of $2 \in \mathbb{Z}_{19}^*$ must divide $\varphi(19) = 18$ and such possible values are $1, 2, 3, 6, 9, 18$.)

Then by Theorem 2.15, as $2 \in \mathbb{Z}_{19}^*$ has multiplicative order 18, 2^m has multiplicative order of $18 \,/ \gcd(m, 18)$, for every $m \in \mathbb{Z}$.

Since we want to find other elements having multiplicative order of 18, $\gcd(m, 18) = 1$ meaning that we are only interested in values of m that are relatively prime with 18, namely $m = \{1, 5, 7, 11, 13, 17\}$. In other words, $2^1, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17}$ are the elements that we are looking for, but since we are in $\mathbb{Z}_{19}$, we have to apply mod 19 on all of them as the last step.

$$2^1 \equiv 2 \pmod{19}, \quad 2^5 \equiv 13 \pmod{19}$$

$$2^7 \equiv 14 \pmod{19}, \quad 2^{11} \equiv 15 \pmod{19}$$

$$2^{13} \equiv 3 \pmod{19}, \quad 2^{17} \equiv 10 \pmod{19}$$

Hence, the set of elements is $\{2, 3, 10, 13, 14, 15\}$.

Problem 2. Exercise 40: Show that if p is an odd prime, with $p \equiv 3 \pmod 4$, then $(\mathbb{Z}_p^*)^4 = (\mathbb{Z}_p^*)^2$. More generally, show that if n is an odd positive integer, when $p \equiv 3 \pmod 4$ for each prime $p|n$, then $(\mathbb{Z}_n^*)^4 = (\mathbb{Z}_n^*)^2$

Solution. This question has **2 parts**.

Part 1: *Show that if p is an odd prime, with $p \equiv 3$ (mod 4), then $(\mathbb{Z}_p^*)^4 = (\mathbb{Z}_p^*)^2$.*

The equivalence of proving that $(\mathbb{Z}_p^*)^4 = (\mathbb{Z}_p^*)^2$ is to show $(\mathbb{Z}_p^*)^4 \subseteq (\mathbb{Z}_p^*)^2$ and $(\mathbb{Z}_p^*)^2 \subseteq (\mathbb{Z}_p^*)^4$.

"$(\mathbb{Z}_p^*)^2 \subseteq (\mathbb{Z}_p^*)^4$:" assuming that we have some arbitrary $\alpha \in (\mathbb{Z}_p^*)^2$, then by definition, $\beta^2 \equiv \alpha \pmod p$, for some $\beta \in \mathbb{Z}_p$. We want to show that this also implies $\gamma^4 \equiv \alpha \pmod p$, for some $\gamma \in \mathbb{Z}_p$.

To this end, we make the following observation: $\beta^2 \equiv \alpha \pmod p \implies 1 \cdot \beta^2 \equiv \alpha \pmod p \implies \beta^{p-1} \cdot \beta^2 \equiv \alpha \pmod p$, since $\varphi(p) = p - 1$ and by Euler's Theorem, $\beta^{\varphi(p)} = \beta^{p-1} \equiv 1 \pmod p$.

Also, $p \equiv 3 \pmod 4$ implies $p = 4x + 3$ for some $x \in \mathbb{Z}$. Thus, by substituting $4x + 3$ to p in the congruence above, we obtain the following: $\beta^{4x+2} \cdot \beta^2 \equiv \alpha \pmod p \implies \alpha \equiv \beta^{4x+4} \pmod p \implies \beta^{4(x+1)} \equiv \alpha \pmod p \implies \beta^{4(x+1)} = (\beta^{x+1})^4 \equiv \alpha \pmod p \implies \gamma^4 \equiv \alpha \pmod p$ for some $\gamma = \beta^{(x+1)}$, and we can easily see that with such choice, γ is in $\mathbb{Z}_p$. Thus, $(\mathbb{Z}_p^*)^2 \subseteq (\mathbb{Z}_p^*)^4$.

"$(\mathbb{Z}_p^*)^4 \subseteq (\mathbb{Z}_p^*)^2$:" this direction is trivial, since we can define $(\mathbb{Z}_p^*)^4$ based on $(\mathbb{Z}_p^*)^2$ as follow $(\mathbb{Z}_p^*)^4 = \{\beta = \alpha^2 \mid \alpha \in (\mathbb{Z}_p^*)^2\}$. In other words, if we have some $\beta \in (\mathbb{Z}_p^*)^4$, then it must be the case that β is the square of some number, namely, $\beta = \alpha^2$ for some $\alpha \in (Z_p^*)^2$. Thus, it's also true that $\beta \in (\mathbb{Z}_p^*)^2$ which implies $(\mathbb{Z}_p^*)^4 \subseteq (\mathbb{Z}_p^*)^2$. (You can apply the same argument as above for this case if you want, but I guess it's not necessary)

Part 2: *More generally, show that if n is an odd positive integer, when $p \equiv 3$ (mod 4) for each prime $p|n$, then $(\mathbb{Z}_n^*)^4 = (\mathbb{Z}_n^*)^2$.*

In this part, instead of considering an odd prime p and $Z*_p$, we will consider an arbitrary odd integer n and show that it also holds that $(\mathbb{Z}_n^*)^4 = (\mathbb{Z}_n^*)^2$.

We can factorize an arbitrary integer n as follows: $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$. For simplicity, let us consider the case where n is only the power of one odd prime, namely, $n = p^e$.

"$(\mathbb{Z}_n^*)^2 \subseteq (\mathbb{Z}_n^*)^4$:" assuming that we have some arbitrary $\alpha \in (\mathbb{Z}_n^*)^2$, then by definition, $\beta^2 \equiv \alpha \pmod n$, for some $\beta \in \mathbb{Z}_p$. We want to show that this also implies $\gamma^4 \equiv \alpha \pmod n$, for some $\gamma \in \mathbb{Z}_n$.

To this end, we make the following observation: $\beta^2 \equiv \alpha \pmod n \implies 1 \cdot \beta^2 \equiv \alpha \pmod n \implies \beta^{p^{e-1}(p-1)} \cdot \beta^2 \equiv \alpha \pmod n$, since $\varphi(n = p^e) = p^{e-1}(p-1)$ and by Euler's Theorem, $\beta^{\varphi(n)} \equiv 1 \pmod n$.

Also, $p \equiv 3 \pmod 4$ implies $p = 4x + 3$ for some $x \in \mathbb{Z}$. Thus, by substituting $4x + 3$ to p in the congruence above, we obtain the following: $\beta^{(4x+3)^{e-1}(4x+2)} \cdot \beta^2 \equiv \alpha \pmod n \implies \alpha \equiv \beta^{4x(4x+3)^{e-1} + 2(4x+3)^{e-1} + 2} \pmod n \implies \beta^{4(x(4x+3)^{e-1} + 1/2((4x+3)^{e-1}+1))} \equiv \alpha \pmod n$.

Observe that $1/2((4x+3)^{e-1}+1)$ is an integer because $(4x+3)^{e-1}$ is an odd number which makes $(4x+3)^{e-1}+1$ an even number. This implies $\gamma^4 \equiv \alpha \pmod{n}$ for some $\gamma = \beta^{x(4x+3)^{e-1}+1/2((4x+3)^{e-1}+1)}$. Thus, $(\mathbb{Z}_n^*)^2 \subseteq (\mathbb{Z}_n^*)^4$.

"$(\mathbb{Z}_n^*)^4 \subseteq (\mathbb{Z}_n^*)^2$:" this direction is trivial (see part 1).

Therefore, $(\mathbb{Z}_n^*)^4 = (\mathbb{Z}_n^*)^2$ for $n = p^e$. The argument also works for any value of p and any exponent e which implies that the statement holds for any arbitrary $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$.

(Some clarification: previously, I wrote $\alpha \equiv \beta^2 \pmod{n}$ in my other notes instead of $\beta^2 \equiv \alpha \pmod{n}$ and all that during my OH. They are both correct, in theory, because $\cdot \equiv \cdot \pmod{n}$ is an equivalence relation so it is transitive. But after staring at the proof a while, I decided to switch since it makes more sense to me...)