QUANTUM ALGORITHMS
HOMEWORK 4 SELECTED SOLUTIONS

PROF. MATTHEW MOORE

AP 2. **(i)** Compute 7^7 in $\mathbb{Z}_4$.

Solution: Since $7 \equiv -1 \pmod 4$, we have

$$7^7 \equiv (-1)^7 \equiv -1 \pmod 4.$$

(ii) Compute 7^{7^7} in $\mathbb{Z}_4$.

Solution: This is quite similar to the previous problem. Since 7^7 is odd, we have

$$7^{7^7} \equiv (-1)^{7^7} \equiv -1 \pmod 4.$$

(iii) Compute $7^{7^{7^7}}$ in $\mathbb{Z}_5$ [*Hint 1: use the previous part and Fermat's little theorem.*] [*Hint 2:* 7^3.]

Solution: Fermat's little theorem for $\mathbb{Z}_5$ is

$$x^4 \equiv 1 \pmod 5 \text{ for } x \not\equiv 0 \pmod 5.$$

$7 \not\equiv 0 \pmod 5$, so the theorem applies in this case. From the previous problem, we know that

$$7^{7^7} \equiv -1 \pmod 4,$$

and since $-1 \equiv 3 \pmod 4$, we have $7^{7^7} = 3 + 4k$. Therefore

$$7^{7^{7^7}} \equiv 7^{3+4k} \equiv 7^3 \cdot (7^4)^k \overset{\text{Fermat}}{\equiv} 7^3 \cdot (1)^k \equiv 7^3 \equiv 2^3 \equiv 8 \equiv 3 \pmod 5.$$

Thus $7^{7^{7^7}} \equiv 3 \pmod 5$.

AP 3. Compute $2^{3^{4^5}}$ mod 79. I suggest that you do this without using a computer. [*Hint:* $78 = 2 \cdot 3 \cdot 13$.]

Solution: 79 is prime, and 2 is coprime to it, so by Fermat's Little Theorem if $3^{4^5} = r + 78k$ then

$$2^{3^{4^5}} = 2^{r+78k} = 2^r 2^{78k} = 2^r \left(2^{78}\right)^k = 2^r \left(1\right)^k = 2^r \pmod{79}.$$

We therefore endeavor to calculate 3^{4^5} modulo 78. Since $78 = 2 \cdot 3 \cdot 13$, we proceed to calculate it in the factors, and then recombine the value. We have

$$3^{4^5} = (1)^{4^5} = 1 \pmod 2, \tag{0.1}$$

$$3^{4^5} = (0)^{4^5} = 0 \pmod 3, \tag{0.2}$$

$$3^{4^5} = 3^{4+12k} = 3^4 = 27 \cdot 3 = 1 \cdot 3 = 3 \pmod{13} \tag{0.3}$$

Date: March 2, 2021.

(line (0.3) is Fermat's Little Theorem again, this time using $4^k = 4 \pmod{12}$). Line (0.1) implies $3^{4^5} = 1 + 2k_1$, so combined with line (0.2) we have

$$1 + 2k_1 = 3^{4^5} = 0 \pmod 3.$$

It follows that $2k_1 = -1 = 2 \pmod 3$, and since 2 is coprime to 3 we have $k_1 = 1 \pmod 3$. Hence $k_1 = 1 + 3k_2$ and

$$3^{4^5} = 1 + 2k_1 = 1 + 2(1 + 3k_2) = 3 + 6k_2.$$

Combined with line (0.3) we have

$$3 + 6k_2 = 3^{4^5} = 3 \pmod{13}.$$

It follows that $6k_2 = 0 \pmod{13}$, and since 6 is coprime to 13 we have $k_2 = 0 \pmod{13}$. Hence $k_2 = 0 + 13k_3$ and

$$3^{4^5} = 3 + 6k_2 = 3 + 6(0 + 13k_3) = 3 + 78k_3.$$

Therefore $3^{4^5} = 3 \pmod{78}$ and

$$2^{3^{4^5}} = 2^{3+78k_3} = 2^3 = 8 \pmod{79}.$$

AP 4. Let $n \in \mathbb{N}$ and define $\varphi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^\times\right|$ (i.e. the number of numbers coprime to n between 1 and n).

(i) Prove that if $\gcd(m, n) = 1$ then $\varphi(m \cdot n) = \varphi(m)\varphi(n)$.

Solution:

Proof. The Chinese Remainder Theorem (from class) states that

$$\left(\mathbb{Z}/mn\mathbb{Z}\right)^\times \cong \left(\mathbb{Z}/m\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$$

when m and n are coprime. It follows that

$$\begin{aligned}\varphi(mn) &= \left|\left(\mathbb{Z}/mn\mathbb{Z}\right)^\times\right| = \left|\left(\mathbb{Z}/m\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/n\mathbb{Z}\right)^\times\right| \\ &= \left|\left(\mathbb{Z}/m\mathbb{Z}\right)^\times\right| \cdot \left|\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\right| = \varphi(m) \cdot \varphi(n)\end{aligned}$$

for coprime m and n, as claimed. □

(ii) Prove that if p is a prime then

$$\varphi(p^k) = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right).$$

Solution:

Proof. If p is prime, then the only numbers which fail to be coprime to p^k are of the form $p^\ell \cdot c$ for $\ell > 0$ and c coprime to p. The distinct residues of these numbers modulo p^k are

$$\underbrace{0, p, 2p, \ldots, (p-1)p}_{p\text{-many}}, \underbrace{p^2, p(p+1), \ldots, p(p+(p-1))}_{p\text{-many}}, 2p^2, \ldots p^{k-1}(p-1)$$

Each block has p elements and there are p^{k-2} blocks, yielding p^{k-1} total distinct residue classes coprime to p^k. Hence

$$\varphi(p^k) = \left|\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times\right| = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right).$$ □

(iii) Use the previous parts to prove that

$$\varphi(n) = n \prod_{\substack{p \text{ prime}, \\ p|n}} \left(1 - \frac{1}{p}\right)$$

(the product is over all prime divisors of n).

Solution:

Proof. If $n = 1$, then $\varphi(n) = 1$ and the formula holds. Assume that $n > 0$ and let $n = p_1^{k_1} \cdots p_m^{k_m}$ be the prime factorization of n with the p_i distinct and $k_i > 0$. From the previous two parts, we have

$$\begin{aligned}\varphi\big(p_1^{k_1} \cdots p_m^{k_m}\big) &= \prod_{i=1}^{m} \varphi\big(p_i^{k_i}\big) = \prod_{i=1}^{m} p_i^{k_i} \left(1 - \frac{1}{p_i}\right) = \big(p_1^{k_1} \cdots p_m^{k_m}\big) \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right) \\ &= n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right) = n \prod_{\substack{p \text{ prime}, \\ p|n}} \left(1 - \frac{1}{p}\right).\end{aligned}$$

□