QUANTUM ALGORITHMS
HOMEWORK 3 SELECTED SOLUTIONS

PROF. MATTHEW MOORE

AP 1. Compute $2^{3^{4^5}} \bmod 79$. If you use a computer to do this, submit your code. There is a way to do this by hand that will almost certainly be faster than a computer, however. [*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

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

$$3^{4^5} = (0)^{4^5} = 0 \pmod{3}, \tag{2}$$

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

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

Date: February 12, 2020.

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

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

(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

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

AP 4. Using the φ function from the previous problem, prove that if x and n are coprime, then

$$x^{\varphi(n)} = 1 \pmod{n}.$$

Explain why this is a generalization of Fermat's Little Theorem.

Solution:

Proof. This result is due to Euler, and is known as *Euler's Theorem*. The function $\varphi()$ from the previous problem is known as *Euler's totient function*.

If x is coprime to n then x is invertible in $\mathbb{Z}/n\mathbb{Z}$ and hence $x \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$. Let k be the order of x. By Lagrange's theorem, k divides $\left|\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\right| = \varphi(n)$, so $\varphi(n) = km$ for some m. Hence

$$1 = 1^m = (x^k)^m = x^{km} = x^{\varphi(n)} \pmod{n}.$$

Observe that if p is a prime then $\varphi(p) = \left|\left(\mathbb{Z}/p\mathbb{Z}\right)^\times\right| = p - 1$, so when recover Fermat's Little Theorem as a special case of this result. □

AP 5. Determine the last 2 digits in the decimal expansion of $2^{3^{4^5}}$ (i.e. the digits in the 1s place and the 10s place).

Solution: The last 2 digits in the expansion is the reside of $2^{3^{4^5}}$ modulo 10^2. Note that 2 and 10^2 are *not* coprime, so AP 4 does not apply directly. We do have, however, that $10 = 2^2 \cdot 5^2$, so we can consider the problem both modulo 2^2 and 5^2.

Let us begin by computing the power modulo 5^2. In this case AP 4 does apply, so have that $2^{\varphi(5^2)} = 1 \pmod{5^2}$, where $\varphi(5^2) = 20$. It is therefore relevant to calculate the exponent 3^{4^5} modulo 20. AP 4 applies again since 3 is coprime to 20, so it will be relevant to calculate 4^5 modulo $\varphi(20) = 8$. We have that $4^2 = 0 \pmod 8$, so $4^5 = 0 \pmod 8$. Therefore $4^5 = 8k$ for some k and hence

$$3^{4^5} = 3^{8k} = \left(3^8\right)^k = \left(3^{\varphi(20)}\right)^k = 1^k = 1 \pmod{20}.$$

Therefore $3^{4^5} = 1 + 20\ell$ for some ℓ, so

$$2^{3^{4^5}} = 2^{1+20\ell} = 2\left(2^{20}\right)^\ell = 2\left(2^{\varphi(25)}\right)^\ell = 2 \cdot 1^\ell = 2 \pmod{25}.$$

Therefore $2^{3^{4^5}} = 2 + 25n$ for some n.

We now consider the calculation modulo 2^2. We have

$$2^{3^{4^5}} = 0 \pmod 4 \qquad \text{and} \qquad 2^{3^{4^5}} = 2 + 25n = 2 + n \pmod 4$$

(the first one follows since 2^2 divides $2^{3^{4^5}}$). Setting these equal and solving for n, we have $n = 2 \pmod 4$, so $n = 2 + 4m$ for some m. Substituting this to the end result of the previous paragraph yields

$$2^{3^{4^5}} = 2 + 25n = 2 + 25(2 + 4m) = 2 + 50 + 100m = 52 + 100m = 52 \pmod{100}.$$

Therefore the first two digits are 52.