Worksheet 10: Binary Exponentiation, Euler's Theorem

Problem 1. Calculate binary representations of the following numbers.

(a) 17

(b) 64

(c) 97

(d) 100

Problem 2. Formulate and prove a rule for determining if a number is divisible by 3 using the digits of the binary representation.

Problem 3. Calculate $\varphi(36000)$.

Solution. Observe that
$$36000 = 36 \cdot 1000 = (2 \cdot 3)^2 \cdot (2 \cdot 5)^3 = 2^5 \cdot 3^2 \cdot 5^3.$$
Thus
$$\varphi(36000) = 2^4 \cdot (2-1) \cdot 3^1 \cdot (3-1) \cdot 5^2 \cdot (5-1) = 16 \cdot 3 \cdot 2 \cdot 25 \cdot 4 = 9600.$$

Problem 4. Find the units digit of 3^{100}.

Solution. Observe that $\varphi(10) = 4$ and that $\gcd(3, 10) = 1$, so by Euler's theorem we have $3^4 \equiv 1 \bmod 10$. Thus
$$3^{100} = (3^4)^{25} \equiv 1^{25} = 1 \bmod 10$$
so the units digit is 1.

Problem 5. Show that $17 \mid 11^{104} + 1$.

Solution. Observe that $\varphi(17) = 16$ since 17 is prime. Moreover, we have $\gcd(11, 17) = 1$. Thus, by Euler's theorem, we have
$$11^{104} = 11^{16 \cdot 6 + 8} = (11^{16})^6 \cdot 11^8 \equiv 11^8 \bmod 17.$$
We now use binary exponentiation to compute $11^8 \bmod 17$. First, $11^2 = 121 \equiv 2 \bmod 17$. Then $11^4 = (11^2)^2 \equiv 2^2 \equiv 4 \bmod 17$. Finally $11^8 \equiv (11^4)^2 \equiv 4^2 = 16 \bmod 17$. Thus
$$11^{104} + 1 \equiv 16 + 1 = 17 \equiv 0 \bmod 17,$$
showing that 11^{104} is divisible by 17.

Problem 6. (a) Show that, if n is odd, then $\varphi(2n) = \varphi(n)$.

(b) Show that, if n is even, then $\varphi(2n) = 2\varphi(n)$.

Solution. Let $n = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorization of n where $e_i \geqslant 1$ for all i. If n is odd, then 2 is not a prime factor of n, so the prime factorization of $2n$ is $2^1 \cdot p_1^{e_1} \cdots p_r^{e_r}$. Thus
$$\varphi(2n) = 2^0 \cdot (2-1) \cdot \varphi(n) = \varphi(n).$$
On the other hand, if n is even, then 2 is already a prime factor of n, so let us say that $p_1 = 2$. Then
$$\varphi(2n) = 2^{(e_i+1)-1} \cdot (2-1) \cdot \varphi(p_2^{e_2} \cdots p_r^{e_r}) = 2\varphi(n).$$

Problem 7. Show that $\phi(n) = n/2$ if and only if $n = 2^e$ for some positive integer e.

Solution. If $n = 2^e$ for some $e \geqslant 1$, then
$$\varphi(n) = 2^{e-1} \cdot (2-1) = 2^{e-1} = n/2,$$
as desired. Conversely, suppose $\varphi(n) = n/2$. By prime factorization, there exists an integer $e \geqslant 0$ and an odd integer $m \geqslant 1$ such that $n = 2^k m$. If $e = 0$, then n is odd, but then $n/2$ is not an integer while $\varphi(n)$ is, and we're at a contradiction. Thus we must have $e \geqslant 1$. We then have
$$2^{e-1} m = \frac{n}{2} = \varphi(n) = \phi(2^e)\varphi(m) = 2^{e-1}\varphi(m).$$
Dividing through my 2^{e-1} shows that $m = \varphi(m)$, which is impossible unless $m = 1$. Thus we must have $n = 2^e$.

Problem 8. Show that, if $\varphi(n) \mid n-1$, then n is square-free (ie, all of the exponents in its prime factorization are 1).

Solution. Suppose n is not square-free. Then there is a prime divisor p of n such that $p^e \mid n$ for some $e \geqslant 2$. But then $p^{e-1} \mid \varphi(n)$, so $p \mid \varphi(n)$, so $p \mid n-1$. This is a contradiction: we must have $\gcd(n-1, n) = 1$.

Problem 9. Suppose $b_0, \dots, b_r \in \{0, 1\}$ with $b_r = 1$ and let $k = b_0 + 2b_1 + 2^2 b_2 + \cdots + 2^r b_r$ be the number whose binary representation is $b_r \cdots b_0$. Write down a formula for the number of multiplications required when computing a^k for some a.

Solution. It requires r squarings, each of which entails a multiplcation, and then the number of multiplications needed to assemble the result is 1 less than the number of 1's in the binary representation. In other words, it requires

$$r + (b_r + \cdots + b_0 - 1).$$

At worst, all of the binary digits are 1, in which case the above expression evaluates to $r + (r + 1 - 1) = 2r$. In other words, no matter what, binary exponentiation with an exponent that has r binary digits will not require more than $2r$ multiplications.

Problem 10. How many prime numbers are there such that p divides $29^p + 1$?

Solution. If $p = 29$, clearly $p \nmid 29^p + 1$. Thus we can assume that $\gcd(p, 29) \equiv 1$. Then $29^{\varphi(p)} = 29^{p-1} \equiv 1 \bmod p$ by Euler's theorem, so $29^p \equiv 29 \bmod p$. Thus

$$29^p + 1 \equiv 29 + 1 \equiv 30 \bmod p.$$

This shows that $p \mid 29^p + 1$ if and only if $p \mid 30$. There are exactly 3 primes dividing 30: namely, 2, 3 and 5.