MA2C03 Mathematics
School of Mathematics, Trinity College
Hilary Term 2016
Lecture 57 (March 30, 2016)

David R. Wilkins

41.8. Computing Powers in Modular Arithmetic

Let m be a positive integer, and let a be an integer. Suppose that one wishes to calculate the value of a^n modulo m, where n is some large positive integer. It is not computationally efficient to calculate the value of a^n for a large value of n and then reduce the value of this integer modulo m.
Instead one may proceed by calculating a sequence

$$a_0, a_1, a_2, a_3, \ldots$$

of integers, where $a_0 \equiv a \pmod{m}$ $0 \leq a_i < m$ and $a_{i+1} \equiv a_i^2 \pmod{m}$ for $i = 0, 1, 2, 3, \ldots$. Now $a^{2^{i+1}} = (a^{2^i})^2$ for all non-negative integers i. It then follows from Lemma 41.9 and the Principle of Mathematical Induction that $a^{2^i} \equiv a_i \pmod{m}$ for all non-negative integers i. Thus the members of the sequence $a_0, a_1, a_2, a_3, \ldots$ are congruent modulo m to those values of a^n for which n is a non-negative power of 2.

Now any positive integer may be expressed as a sum of powers of two. Indeed let n be a positive integer, and let the digits in the standard binary representation of n, read from right to left, be $e_0, e_1, \ldots, e_r$, where e_0 is the least significant digit, e_r is the most significant digit, and e_i is equal either to 0 or to 1 for $i = 0, 1, \ldots, r$. Then $n = \sum_{i=0}^{k} e_i 2^i$, and thus n is the sum of those powers 2^i of two for which $e_i = 1$.

Let $n = 2^{k_1} + 2^{k_2} + \cdots 2^{k_m}$, where $k_1, k_2, \ldots, k_m$ are distinct non-negative integers. Then $a^n = a^{2^{k_1}} a^{2^{k_2}} \cdots a^{2^{k_m}}$. It then follows from Lemma 41.9 that $a^n \equiv a_{k_1} a_{k_2} \cdots a_{k_m} \pmod{m}$, where $0 \leq a_i < m$ and $a_i \equiv a^{2^i} \pmod{m}$ for all non-negative integers i.

Example

We calculate $58^n \pmod{221}$ where

$$\begin{aligned} n &= 2^{176} \\ &= 95780971304118053647396689196894323976171195136475136. \end{aligned}$$

Let $a_0 = 58$ and let $0 \leq a_{i+1} < 221$ and $a_{i+1} \equiv a_i^2 \pmod{221}$ for all non-negative integers i. Then

$$a_0 = 58,\ \ a_1 = 49,\ \ a_2 = 191,\ \ a_3 = 16,\ \ a_4 = 35,\ \ a_5 = 120, a_6 = 35.$$

Note that $a_4 = a_6$. The definition of the numbers a_i then ensures that $a_{4+j} = a_{6+j}$ for all non-negative integers. It follows from this that $a_i = 35$ when i is even and $i \geq 4$, and $a_i = 120$ when i is odd and $i \geq 5$. In particular $58^n \equiv 35 \pmod{221}$ when $n = 2^{176}$, since $58^n \equiv a_{176} \pmod{221}$ and $a_{176} = 35$.

Let m be a positive integer, let a be an integer satisfying $0 \leq a < m$, and let the infinite sequence $a_0, a_1, a_2, a_3, \ldots$ of integers be defined such that $a_0 = a$, $0 \leq a_{i+1} < m$ and $a_{i+1} \equiv a_i^2 \pmod{m}$ for all non-negative integers i. Now the integers a_i can only take on m possible values. It follows that there must exist a non-negative integer r and a strictly positive integer p such that $a_r = a_{r+p}$. But it then follows from the definition of the integers a_i that $a_{r+j} = a_{r+p+j}$ for all non-negative integers j. A straightforward proof by induction on k shows that $a_{r+kp+j} = a_{r+j}$ for all non-negative integers j and k. Thus the values of the sequence $a_r, a_{r+1}, a_{r+2}, \ldots$ are periodic, with period equal to or dividing p, and therefore the values of a_i for $i \geq r$ are completely determined by the values of a_i for $r \leq i < r + p$.

Example

We consider the value of $1234^n \pmod{13039}$ for some large integer values of n. We define a sequence $a_0, a_1, a_2, a_3, \ldots$ of integers satisfying $0 \leq a_i < 13039$, where $a_0 = 1234$ and $a_{i+1} \equiv a_i^2 \pmod{13039}$. Calculations show that $a_4 = a_{32} = 10167$. However $a_i \neq 10167$ when $4 < i < 32$. Therefore the sequence of values a_i for $i \geq 4$ is periodic, with period 28, so that $a_{i+28k} = a_i$ for all non-negative integers i and k with $i \geq 4$. The values of a_i for all non-negative integers i are thus determined by the values of a_i for which $0 \leq i < 32$.

We now calculate the value of $1234^n \pmod{13039}$ when

$$n = 188986894442529239859 20.$$

Now $n = 2^{47} + 2^{63} + 2^{74}$. It follows that $1234^n \equiv a_{47}a_{63}a_{74} \pmod{13039}$. Moreover $a_{47} = a_{19} = 11935$, $a_{63} = a_7 = 3758$ and $a_{74} = a_{18} = 2211$. Now $11935 \times 3758 \times 2211 \equiv 12377 \pmod{13039}$. We conclude therefore that $1234^n \equiv 12377 \pmod{13039}$. We note also $1234^n > 2^{10n}$. It is not feasable to write out or print the binary or decimal representation of such a large number!