Remainders of $Aa^x + Bx$

Yimin Ge
Vienna, Austria

Abstract

In recent times, a class of number theoretic problems became quite popular at various competitions, namely analysing the remainders of $a^x + bx$ modulo some positive integer m. In this note, I will try to unite these problems to a more general statement.

We will start with a very fundamental theorem about quadratic residues and although we won't need it in this note, the key idea of its proof can be adapted to many problems and we will make use of it throughout this article.

Theorem 1. Let p be an odd prime number, k a positive integer and a any integer not divisible by p. Then a is a quadratic residue modulo p^k if and only if a is a quadratic residue modulo p.

Proof. The "*only if*"-part is trivial, so we will only prove the "*if*"-part.

The proof goes by induction on k: Suppose that a is a quadratic residue modulo p^k. We will show that it is a quadratic residue modulo p^{k+1}.

By the induction hypothesis, there exists an integer x so that $x^2 \equiv a \pmod{p^k}$, so there exists an integer l so that $x^2 = a + lp^k$. Clearly $p \nmid x$. Take $x' = x + y \cdot p^k$ for some integer y. We shall prove that there exists an integer y so that $x'^2 \equiv a \pmod{p^{k+1}}$.

We have

$$\begin{aligned} x'^2 &= (x + yp^k)^2 = x^2 + 2xyp^k + y^2p^{2k} \\ &= a + lp^k + 2xyp^k + y^2p^{2k} \equiv a + lp^k + 2xyp^k \pmod{p^{k+1}} \end{aligned}$$

so it remains to be proven that there exists an integer y so that

$$lp^k + 2xyp^k \equiv 0 \pmod{p^{k+1}} \quad \Leftrightarrow \quad l + 2xy \equiv 0 \pmod{p}.$$

But this congruence is solvable in y since it is a linear congruence in y and $\gcd(2x, p) = 1$. □

The key idea in the proof above was a very useful trick: Using induction on the module m, we construct a new solution x' modulo the induction-stepped module m' from the old solution x modulo m by adding a variable parameter y. Notice that x' remains invariant modulo m by varying y. It remains to be proven that an appropriate y can be found.

The following problem appeared at the Brazilian National Olympiad in 2005:

Problem 1 (Brazil 2005)**.** *Given positive integers a, b and c, prove that there exists a positive integer x such that*

$$a^x + x \equiv b \pmod{c}.$$

A special case of this problem appeared on the IMO Shortlist of 2006:

Problem 2 (IMO Shortlist 2006)**.** *For all positive integers n, show that there exists a positive integer m such that n divides $2^m + m$.*

A similar problem was given at the USA Team Selection Test in 2007:

Problem 3 (USA 2007)**.** *Determine whether or not there exist positive integers a and b such that a does not divide $b^n - n$ for all positive integers n.*

All these problems can be generalized to the following statement:

Theorem 2. Let A, a, B be integers and let M be a positive integer. Then there exists a positive integer x for every integer C so that

$$Aa^x + Bx \equiv C \pmod{M}$$

if and only if $\gcd(B, M) = 1$.

Note that another wording of this statement would be: $\{Aa^x + Bx \bmod m \mid x \in \mathbb{Z}^+\} = \{0, \ldots, M-1\}$ if and only if $\gcd(B, M) = 1$.

The "*only if*"-part is easy: suppose that p is a common prime divisor of B and M. If $p \mid Aa$ take $C = 1$, otherwise take $C = 0$. We see that $Aa^x + Bx \equiv C \pmod{p}$ cannot be fulfilled this way.

I will give two proofs of the "*if*"-part:

Proof 1. Suppose that $\gcd(B, M) = 1$. Let C be any integer and let $M = mn$ ($m, n \in \mathbb{Z}^+$) so that every prime divisor of n divides a and $\gcd(m, a) = \gcd(m, n) = 1$ (that is, if $a = q_1^{\alpha_1} \ldots q_s^{\alpha_s} \cdot a'$ and $M = q_1^{\beta_1} \ldots q_s^{\beta_s} \cdot m$ with $q_i \nmid a'$ and $q_i \nmid m$, take $n = q_1^{\beta_1} \ldots q_s^{\beta_s}$). Then $n \mid a^x$ for sufficiently large x. We have

$$Aa^x + Bx \equiv C \pmod{M}$$

if and only if

$$Aa^x + Bx \equiv C \pmod{m} \quad \text{and} \quad Aa^x + Bx \equiv C \pmod{n}.$$

Since $\gcd(B, n) = 1$, there exists a positive integer B' so that $BB' \equiv 1 \pmod{n}$. We see that any sufficiently large x with $x \equiv B'C \pmod{n}$ satisfies

$$Aa^x + Bx \equiv C \pmod{n}. \tag{1}$$

Let $x = yn + B'C$. We shall prove that there exists a sufficiently large integer y so that

$$Aa^x + Bx \equiv C \pmod{m}. \tag{2}$$

This is equivalent to

$$\begin{aligned} Aa^{yn+B'C} + B(yn+B'C) &\equiv C \pmod{m} \\ \Leftrightarrow (Aa^{B'C})a^{ny} + (Bn)y + (BB'C - C) &\equiv 0 \pmod{m} \\ \Leftrightarrow c \cdot e^y + by + t &\equiv 0 \pmod{m} \end{aligned}$$

where $c = (Aa^{B'C}), e = a^n, b = Bn, t = BB'C - C$. We clearly have $\gcd(e,m) = \gcd(b,m) = 1$.

Let $f(y) = ce^y + by + t$. We will now work with induction on m.

For $m = 1$, there is nothing left to prove. Suppose that $m > 1$ and assume that the statement is true for every $m' < m$. Let p be the largest prime divisor of m and let $m = p^k p_1^{k_1} \dots p_r^{k_r}$ be the prime factorization of m. Let $m' = p^{k-1} p_1^{k_1} \dots p_r^{k_r}$. By the induction hypothesis, there exists a positive integer y so that

$$f(y) \equiv 0 \pmod{m'},$$

thus there exists an integer l so that $f(y) = lm'$. Take

$$y' = y + z \cdot (p-1)p^{k-1} \prod_{i=1}^{r} (p_i - 1)p^{k_i}$$

for some positive integer z. We shall prove that there exists a z so that $f(y') \equiv 0 \pmod{m}$.

We have

$$\begin{aligned} f(y') &= ce^{y + z\cdot(p-1)p^{k-1}\prod_{i=1}^{r}(p_i-1)p_i^{k_i}} + b(y + z \cdot (p-1)p^{k-1}\prod_{i=1}^{r}(p_i-1)p_i^{k_i}) + t \\ &= ce^y \cdot \underbrace{e^{z\cdot(p-1)p^{k-1}\prod_{i=1}^{r}(p_i-1)p_i^{k_i}}}_{\equiv 1 \text{ mod } m \text{ by Euler's theorem}} + by + t + z \cdot b(p-1)p^{k-1}\prod_{i=1}^{r}(p_i-1)p_i^{k_i} \\ &\equiv (ce^y + by + t) + z \cdot b(p-1)p^{k-1}\prod_{i=1}^{r}(p_i-1)p_i^{k_i} \\ &= lm' + z \cdot bm'(p-1)\prod_{i=1}^{r}(p_i - 1) \pmod{m}. \end{aligned}$$

Hence, we have to prove that

$$lm' + z \cdot bm'(p-1)\prod_{i=1}^{r}(p_i-1) \equiv 0 \pmod{m}.$$

has a positive integral solution z. Dividing this congruence (including the module m) by m', we obtain the equivalent congruence

$$l + z \cdot b(p-1)\prod_{i=1}^{r}(p_i-1) \equiv 0 \pmod{p}$$

and this congruence is solveable since it is a linear congruence in z and

$$\gcd(b(p-1)\prod_{i=1}^{r}(p_i-1),p)=1,$$

so the induction step is complete.

We have proved now that there exists a positive integer y so that $f(y)\equiv 0 \pmod{m}$, so there exists an x so that (2) is satisfied. We still have to prove that we can choose y sufficiently large so that (1) is satisfied. But this is evidential since if y is a solution of $f(y)\equiv 0 \pmod{m}$, then so is $y+\lambda\cdot m\varphi(m)$ for every $\lambda\in\mathbb{Z}^+$. This completes our proof. □

Proof 2. As in proof 1 suppose that $\gcd(B,M)=1$ and let C be any integer. Consider the sequence $Aa^1, Aa^2,\dots$ which will eventually become periodic modulo M. Let T be the minimal length of the period, i.e. the smallest positive integer so that $Aa^{x+kT}\equiv Aa^x \pmod{M}$ for all sufficiently large x.

Let $d=\gcd(T,M)$. We will first prove that $d<M$ for $M>1$.

Since $d\mid M$, we have $d\le M$. Suppose that $d=M$. Then $M\mid T$, so in particular, $T\ge M$. However, T cannot exceed M since every residue class modulo M can only appear at most once in a minimal cycle of Aa^i, so $M=T$. This implies that every remainder modulo M appears in the cycle so in particular, there exists a positive integer X so that $Aa^X\equiv 0 \pmod{M}$ and thus $Aa^x\equiv 0 \pmod{M}$ for every $x\ge X$. It follows that $T=1$, so $M=1$.

We will now use induction on our claim. $M=1$ is trivial, for $M>1$ we can assume that the statement is true for every $m<M$, so in particular, the statement is true for d. Thus, by the induction hypothesis, there exists a positive integer x so that

$$Aa^x+Bx\equiv C \pmod{d},$$

so $Aa^x+Bx=C+ld$ for some integer l. Setting $x'=x+kT$ for some positive integer k, we have

$$\begin{aligned}Aa^{x'}+Bx' &= Aa^{x+kT}+Bx+k\cdot BT\\ &\equiv (Aa^x+Bx)+k\cdot BT\\ &= C+ld+k\cdot BT \pmod{M}\end{aligned}$$

so it remains to be proven that the congruence

$$ld+k\cdot BT\equiv 0 \pmod{M}$$

has a solution in $k\in\mathbb{Z}^+$. However, dividing this congruence by d (including the module M), we obtain the equivalent congruence

$$l+k\cdot B\frac{T}{d}\equiv 0 \pmod{\frac{M}{d}}$$

which obviously has a solution in k since $\gcd\left(B\frac{T}{d},\frac{M}{d}\right)=1$. This completes our induction step and thus our proof. □