Michigan Math. J. 64 (2015), 655–672

Congruences with Intervals and Subgroups Modulo a Prime

Marc Munsch & Igor E. Shparlinski

Abstract. We obtain new results about the representation of almost all residues modulo a prime p by a product of a small integer and also an element of small multiplicative subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$. These results are based on some ideas, and their modifications, of a recent work of Cilleruelo and Garaev (2014).

1. Introduction

It is well known that the progress on many classical and modern number-theoretic questions depends on the existence asymptotic formulas and good upper and lower bounds on the number of solutions to the congruences of the form

$$au \equiv x \pmod{m}, \tag{1}$$

where u runs through a multiplicative subgroup $\mathcal{G}$ of the group of units $\mathbb{Z}_m^*$ of the residue ring $\mathbb{Z}_m$ modulo an integers $m \geq 2$, and x runs through a set $\{A+1, \dots, A+H\}$ of H consecutive integers; see [17] for an outline of such questions. In the special case where $m = p$ is a prime number and $\mathcal{G}$ is a group of squares, this is a celebrated question about the distribution of quadratic residues.

Recently, various modifications of the congruence (1) have been studied, such as congruences with elements from more general sets than subgroups on the left-hand side and also with products and ratios of variables from short intervals on the right-hand side; see [2; 3; 5; 6; 7; 8; 9; 10; 11; 12; 14; 18] and references therein. New applications of such congruences have also been found and include questions about

- nonvanishing of Fermat quotients [1],
- estimating fixed points of the discrete logarithm [2; 3],
- distribution of pseudopowers [4], and
- distribution of digits in reciprocals of primes [22].

Here we consider the congruence (1) in the special case where $m = p$ is prime. Furthermore, we are mostly interesting in the solvability of (1) for rather small intervals and subgroups.

Since we consider congruences modulo primes, it is convenient to use the language of finite fields.

Received December 8, 2014. Revision received May 13, 2015.

During the preparation of this work, M. Munsch was supported by a postdoctoral grant in CRM of Montreal under the supervision of Andrew Granville and Dimitris Koukoulopoulos, and I. E. Shparlinski was supported in part by the Australian Research Council Grant DP140100118.