DE GRUYTER
OPEN

TATRA MOUNTAINS
Mathematical Publications
DOI: 10.1515/tmmp-2015-0044
Tatra Mt. Math. Publ. **64** (2015), 93–99

NEW SOLVABILITY CONDITIONS FOR CONGRUENCE $ax \equiv b \pmod{n}$

Štefan Porubský

Dedicated to the memory of an unforgettable friend Kaz Szymiczek (1939–2015)

Abstract. K. Bibak *et al.* [arXiv:1503.01806v1 [math.NT], March 5 2015] proved that congruence $ax \equiv b \pmod{n}$ has a solution x_0 with $t = \gcd(x_0, n)$ if and only if $\gcd\left(a, \frac{n}{t}\right) = \gcd\left(\frac{b}{t}, \frac{n}{t}\right)$ thereby generalizing the result for $t = 1$ proved by B. Alomair *et al.* [J. Math. Cryptol. **4** (2010), 121–148] and O. Grošek *et al.* [*ibid.* **7** (2013), 217–224]. We show that this generalized result for arbitrary t follows from that for $t = 1$ proved in the later papers. Then we shall analyze this result from the point of view of a weaker condition that $\gcd\left(a, \frac{n}{t}\right)$ only divides $\gcd\left(\frac{b}{t}, \frac{n}{t}\right)$. We prove that given integers $a, b, n \geq 1$ and $t \geq 1$, congruence $ax \equiv b \pmod{n}$ has a solution x_0 with t dividing $\gcd(x_0, n)$ if and only if $\gcd\left(a, \frac{n}{t}\right)$ divides $\gcd\left(\frac{b}{t}, \frac{n}{t}\right)$.

Gauß revolutionized the number theory with the idea of the congruence in his D. A. He introduced congruence in the very first article of D. A., and the following basic result on the solvability of linear congruence[1]

$$ax \equiv b \pmod{n} \tag{1}$$

which belongs to standard requisites of elementary number theory can be found in Arts. 29, 30 of D. A. (cf. [4]):[2]

Lemma 1. *If $a, b, n \in \mathbb{Z}$, and $\gcd(a, n) = d$, then the congruence* (1) *is solvable if and only if $d | b$.*

2010 Mathematics Subject Classification: Primary 11A07; Secondary 11D04, 11D45, 11A25, 11B50.
Keywords: linear congruence, the greatest common divisor, number of solutions.
The author was supported by the Grant Agency of the Czech Republic, Grant # P201/12/2351, the Mobility grant 7AMB14SKXXX and the strategic development financing RVO 67985807.

[1] In what follows $\mathbb{Z}$ will denote the ring of integers. To simplify the wording and notation all moduli and divisors will be always assumed to be positive in what follows.

[2] For the history of the related linear Diophantine equation $ax + ny = b$ consult, e.g., [3, Chapter II].

It is a bit surprising that Alomair et al. [1, Lemma 3.1] only recently noticed the result given in following Proposition 1 which, as it seems, has not appeared explicitly in the literature before, and which they used in a construction of a hash function. Nevertheless, forerunners of this result could be already found in various hidden forms earlier. One such result can be found in Lemma 2 which we shall use in what follows.

Proposition 1. *Given $a, b \in \mathbb{Z}$, $a \neq 0$, such that $\gcd(a, n) = d|b$, there exists a solution to congruence* (1) *which is coprime to n if and only if*

$$\gcd\left(\frac{b}{d}, \frac{n}{d}\right) = 1,$$

or equivalently, if and only if

$$\gcd(b, n) = \gcd(a, n).$$

In [5] a short proof and a quantitative extension of Proposition 1 is given. In [7] its generalization based on an idempotent analysis of the semigroup of the residue class ring modulo n can be found. In [2, Theorem 3.1] the result of Proposition 1 was generalized to

Proposition 2. *Let $a, b, n \geq 1$ and $t \geq 1$ be given integers. Then congruence* (1) *has a solution x_0 with $\gcd(x_0, n) = t$ if and only if*

$$\gcd\left(a, \frac{n}{t}\right) = \gcd\left(\frac{b}{t}, \frac{n}{t}\right). \tag{2}$$

In this note we shall shortly analyze the validity of Proposition 2 under a weaker condition that

$$\gcd\left(a, \frac{n}{t}\right) \Bigg| \gcd\left(\frac{b}{t}, \frac{n}{t}\right) \tag{3}$$

for some t dividing $\gcd(b, n)$. Then we show that Proposition 2 actually follows from Proposition 1 thereby giving a shorter proof than the original one in [2].

The following elementary result (cf. [8, Lemma 2.1], [6, Lemma2.1] or [7, Corollary 4]) will be used in what follows:

Lemma 2. *If $n, x \in \mathbb{Z}$ and $t = \gcd(n, x)$, then there exists an integer a coprime to n such that*

$$x \equiv ta \pmod{n}.$$

Notice that decomposition $x = t\frac{x}{t}$ does not yield a representation given in previous Lemma 2 in general. Take for instance, $n = 12$ and $x = 9$.

Then $\gcd(12,9) = 3$. Since $\gcd\left(\frac{9}{3}, 12\right) \neq 1$, product $9 = 3 \cdot 3$ is not the representation of $x = 9$ in the spirit of Lemma 2. From incongruent mod 12 solutions 3, 7, 11 to congruence $3 \equiv a \pmod{4}$ only 7, 11 are coprime to 12. Thus only representations $3 \cdot 7$ or $3 \cdot 11$ fulfil the statement of Lemma 2.

The next reformulation of the Gauß solvability condition given in Lemma 1 can be deduced in turn

Lemma 3. *If $a, b, n \in \mathbb{Z}$, then congruence* (1) *is solvable if and only if*

$$\gcd(a,n) \mid \gcd(b,n).$$

The necessary condition of Proposition 2 can be modified in the spirit of the previous Lemma 3 as follows

Proposition 3. *Let $a, b, n \in \mathbb{Z}$. If congruence* (1) *has a solution x_0, then* (3) *holds with $t = \gcd(x_0, n)$.*

Proof. Suppose that x_0 is a solution to (1) and tx_1 with $\gcd(x_1, n) = 1$ is a representation of x_0 as it is given in Lemma 2. Then $t \mid b$ and x_1 solves the congruence

$$ax_1 \equiv \frac{b}{t} \pmod{\frac{n}{t}}. \tag{4}$$

Lemma 3 finishes the proof. □

Notice that a solvability of (1) implies more than simple divisibility relation (3).

Indeed, if x_0 is a solution of (1) and $x_0 = tx_1$ is a representation of this x_0 in the spirit of Lemma 2 with $\gcd(x_1, n) = 1$, then x_1 solves (4) and (4) together with $\gcd(x_1, n) = 1$ imply that $\gcd\left(\frac{b}{t}, \frac{n}{t}\right)$ divides a, and consequently $\gcd\left(\frac{b}{t}, \frac{n}{t}\right)$ also divides $\gcd\left(a, \frac{n}{t}\right)$. This shows that even the reverse divisibility

$$\gcd\left(\frac{b}{t}, \frac{n}{t}\right) \,\Big|\, \gcd\left(a, \frac{n}{t}\right)$$

to that of (3) is also true for $t = \gcd(x_0, n)$ if (1) has a solution x_0. In other words, if (1) is solvable, then (2) holds with $t = \gcd(x_0, n)$.

If (1) is solvable, then $t = \gcd(x_0, n)$ divides b for every solution x_0 to (1). However the necessary condition $t \mid \gcd(b, n)$ for possible candidates t with $t = \gcd(x_0, n)$ is too generous. For instance, congruence $18x \equiv 12 \pmod{24}$ has no solution divisible by $t = 4$. The set of solutions to this congruence is $\{2, 6, 10, 14, 18, 22\}$, and neither of them is divisible by 4. Another example is congruence $x \equiv 2 \pmod{4}$ not possessing solutions coprime to 4 which would correspond to divisor $t = 1$.

Now we show that relation (3) is also sufficient for the solvability of (1), however with a weaker binding between the t's and solutions, as the next result shows:

Proposition 4. *Let $a, b, n \in \mathbb{Z}$. If* (3) *holds for a $t \mid \gcd(b,n)$, then congruence* (1) *has a solution x_0 with $t \mid x_0$.*

Proof. Condition (3) implies that congruence

$$ax \equiv \frac{b}{t} \pmod{\frac{n}{t}} \quad \text{is solvable.}$$

If x_1 is one of its solutions, then $x_1 t$ solves the original congruence (1). □

It can be also noted that a mere solvability of (1) provided (3) holds for an arbitrary t dividing $\gcd(b,n)$ can be proved via Lemma 3 in several different ways. Here are two of them:

The first method. We prove that if for a t dividing $\gcd(b,n)$ condition (3) is satisfied, then always $\gcd(a,n) \mid \gcd(b,n)$. Suppose on the contrary that there is a prime p and a positive integer α such that

$$p^\alpha \mid \gcd(a,n),\, p^{\alpha+1} \nmid \gcd(a,n) \quad \text{while } p^\alpha \nmid b.$$

Let $a = p^\alpha a_1$, $n = p^\alpha n_1$, where $p \nmid a_1$ or $p \nmid n_1$. Let $b = p^\beta b_1$, where $p \nmid b_1$, $\beta \geq 0$ and $\alpha > \beta$. Then $\gcd(b,n) = p^\beta \gcd(b_1, p^{\alpha-\beta} n_1)$ and (3) can be rewritten in the form

$$\gcd\left(p^\alpha a_1, \frac{p^\alpha n_1}{t}\right) \Bigg| \gcd\left(\frac{p^\beta b_1}{t}, \frac{p^\alpha n_1}{t}\right).$$

If $p \nmid t$, then p^α divides the LHS of (3) but not its RHS. Thus $t = p^\gamma t_1$ with $p \nmid t_1$ and $0 < \gamma < \alpha$. Then

$$\gcd\left(p^\alpha a_1, \frac{p^\alpha n_1}{p^\gamma t_1}\right) = p^{\alpha-\gamma} \gcd\left(p^\gamma a_1, \frac{n_1}{t_1}\right),$$

and

$$\gcd\left(\frac{p^\beta b_1}{t}, \frac{p^\alpha n_1}{t}\right) = p^{\beta-\gamma} \gcd\left(\frac{b_1}{t_1}, p^{\alpha-\beta} \frac{n_1}{t_1}\right).$$

Since $p \nmid b_1$, $p^{\beta-\gamma}$ is the highest power of p which divides the RHS of (3).

To finish the proof consider the following two cases:

$p \nmid n_1$: Then $p^{\alpha-\gamma}$ is the highest power of p which divides the LHS of (3), and (3) implies $a - \gamma \leq b - \gamma$, i.e., $\alpha \leq \beta$, what is impossible.

$p \mid n_1$: In this case the highest power of p dividing the LHS of (3) is $p^{\alpha-\gamma+\omega}$ for some positive integer ω. Then (3) implies $\alpha - \gamma + \omega \leq \beta - \gamma$, or $\alpha + \omega \leq \beta$, what is again impossible and the solvability condition $\gcd(a,n) \mid \gcd(b,n)$ follows. □

T h e s e c o n d m e t h o d. The greatest common divisor possesses the following multiplicative property

$$\gcd(ah, bk) = \\ \gcd(a,b)\gcd(h,k)\gcd\left(\frac{a}{\gcd(a,b)}, \frac{k}{\gcd(h,k)}\right)\gcd\left(\frac{b}{\gcd(a,b)}, \frac{h}{\gcd(h,k)}\right). \quad (5)$$

Consequently for every $t \mid n$ we have

$$\gcd(a,n) = \gcd\left(a\cdot 1, \frac{n}{t}\cdot t\right) = \gcd\left(a, \frac{n}{t}\right)\cdot\gcd\left(\frac{a}{\gcd\left(a,\frac{n}{t}\right)}, t\right). \quad (6)$$

Since t also divides b, then the first gcd on the RHS divides $\gcd\left(\frac{b}{t}, \frac{n}{t}\right)$ due to (3) while the second one divides t. Consequently the RHS of (6) divides their mutual product $\gcd(b,n)$, that is $\gcd(a,n) \mid \gcd(b,n)$. □

There follows from the proofs above that parameter t divides $\gcd(x_0, n)$, where x_0 is a solution to (1). This gives the following companion to Proposition 2.

Theorem 1. *Let $a, b, n \geq 1$ and $t \geq 1$ be given integers. Then congruence* (1) *has a solution x_0 with $t \mid \gcd(x_0, n)$ if and only if* (3) *holds with this t.*

We show now that Proposition 1 implies Proposition 2.

Congruence (1) is solvable and an x_0 with $\gcd(x_0, n) = t$, $x_0 = tx_1$ with $\gcd\left(x_1, \frac{n}{t}\right) = 1$ is its solution, if and only if (4) has a solution x_1 coprime to its modulus $\frac{n}{t}$. Proposition 1 shows that this can happen if and only if

$$\gcd\left(a, \frac{n}{t}\right) = \gcd\left(\frac{b}{t}, \frac{n}{t}\right) \qquad \text{as Proposition 2 claims.}$$

All above results remain true verbatim without any change of arguments in an arbitrary commutative principal ideal domain. Typical example besides the ring of rational integers is the ring of Gaußian integers $a + bi$ with $a, b \in \mathbb{Z}$, or more generally, the rings of algebraic integers with the class number 1.

Finally, let us add that in the case of coprime solutions it is proved in [5] that the number of incongruent coprime solutions is given by the following rule:

> *If $\gcd(a,n) = \gcd(b,n) = d$, then there are exactly $\frac{d}{\delta}\varphi(\delta)$ incongruent solutions of* (1) *coprime to n, where δ is the largest divisor of d with $\gcd(\delta, \frac{n}{d}) = 1$, and $\varphi(m)$ is the number of integers $k, 1 \leq k \leq m$, coprime to m.*

On the other side, in [2] it is proved that the number of incongruent solutions x_0 modulo n to (1) with $t = \gcd(x_0, n)$ is given by

$$\frac{\varphi\left(\frac{n}{t}\right)}{\varphi\left(\frac{n}{t\gcd\left(\frac{b}{t},\frac{n}{t}\right)}\right)} = d \prod_{\substack{p \mid d \\ p \nmid \frac{n}{td}}} \left(1 - \frac{1}{p}\right). \quad (7)$$

This gives for the number of coprime incongruent solutions modulo n to (1) the formula

$$\frac{\varphi(n)}{\varphi\left(\frac{n}{d}\right)}. \tag{8}$$

That the numbers for coprime solutions given by these two different formulae coincide, i.e., that

$$\frac{d}{\delta}\varphi(\delta) = \frac{\varphi(n)}{\varphi\left(\frac{n}{d}\right)}$$

can be shown as follows: The equality above reduces to

$$\frac{d}{\delta} = \frac{\varphi(n)}{\varphi\left(\frac{n}{d}\right)\varphi(\delta)}.$$

Here, $\frac{n}{d}$ and δ are coprime, and therefore

$$\varphi\left(\frac{n}{d}\right)\varphi(\delta) = \varphi\left(\frac{n\delta}{d}\right).$$

Since n and $\frac{n\delta}{d}$ have the same prime divisors, the formula

$$\varphi(m) = m\prod_{p|m}\left(1-\frac{1}{p}\right) \quad \text{implies that} \quad \frac{\varphi(n)}{\varphi\left(\frac{n}{d}\right)\varphi(\delta)} = \frac{n}{\frac{n\delta}{d}} = \frac{d}{\delta},$$

as it is claimed.

Finally, notice that also the number of solutions x_0 to (1) given in [2] follows from the formula giving the number of coprime solutions.

Really, as we have mentioned above there is one to one correspondence between incongruent solutions x_0 modulo n to (1) with $t = \gcd(x_0, n)$ and incongruent solutions x_1 modulo $\frac{n}{t}$ to (4) satisfying condition $\gcd\left(x_1, \frac{n}{t}\right) = 1$. Relation (8) implies that the number of the later ones is

$$\frac{\varphi\left(\frac{n}{t}\right)}{\varphi\left(\frac{n}{t\gcd\left(\frac{b}{t},\frac{n}{t}\right)}\right)} \quad \text{which is just (7).}$$

Acknowledgement. The author thanks Professor O. G r o š e k for calling his attention to manuscript [2] and Professor O. S t r a u c h for stimulating discussions.

REFERENCES

[1] ALOMAIR, B.—CLARK, A.—POOVENDRAN, R.: *The power of primes: security of authentication based on a universal hash-function family*, J. Math. Cryptol. **4** (2010), 121–148.

[2] BIBAK, K.—KAPRON, B. M.—SRINIVASAN, V.—TAURASO, R.—TÓTH, L.: *Restricted linear congruences and an authenticated encryption scheme*, arXiv:1503.01806v1 [math.NT], March 5, 2015.

[3] DICKSON, L. E.: *History of the Theory of Numbers. Vol. II. Diophantine Analysis*. Carnegie Institution of Washington, New York, 1920.

[4] GAUSS, C.-F.: *Disquisitiones Arithmeticae*. Transl. from the Latin by Arthur A. Clarke, Rev. by William C. Waterhouse, with the help of Cornelius Greither and A. W. Grootendorst. (Reprint of the 1966 ed.). Springer-Verlag, New York, 1986.

[5] GROŠEK, O.—PORUBSKÝ, Š.: *Coprime solutions to* $ax \equiv b \pmod{n}$, J. Math. Cryptol. **7** (2013), 217–224.

[6] LAŠŠÁK, M.—PORUBSKÝ, Š.: *Fermat-Euler theorem in algebraic number fields*, J. Number Theory **60** (1996), 254–290.

[7] PORUBSKÝ, Š.: *Idempotents and Congruence* $ax \equiv b \pmod{n}$. in: From Arithmetic to Zeta-Functions. Number Theory in Memory of Wolfgang Schwarz. (Jürgen Sander, Jörn Steuding and Rasa Steuding, Eds.), Springer Verlag, 2016 (to appear).

[8] SCHWARZ, Š.: *The role of semigroups in the elementary theory of numbers*, Math. Slovaca **31** (1981), 369–395.

Received November 22, 2015

Institute of Computer Science
Academy of Sciences of the Czech Republic
Pod Vodárenskou věží 2
182 07 Praha 8–Libeň
CZECH REPUBLIC

E-mail: sporubsky@hotmail.com