CERIAS Tech Report 2007-84

Protocols and Systems for Privacy Preserving Protection of Digital Identity

by Abhilasha Bhargav-Spantzel
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

Congruences for $r_s(n)$ Modulo $2s$

Samuel S. Wagstaff, Jr.

Department of Computer Science and Center for Education and Research in Information Assurance and Security, 1315 Recitation Building, Purdue University, West Lafayette, IN 47907-1315, USA

Abstract

We determine $r_s(n)$ modulo $2s$ when s is a prime or a power of 2. For general s, we prove a congruence for $r_s(n)$ modulo the largest power of 2 dividing $2s$.

Key words: Sums of squares, congruence.

Let $r_s(n)$ denote the number of ways to write an integer n as the sum of s squares of integers, that is, $r_s(n)$ is the number of solutions to

$$n = x_1^2 + x_2^2 + \cdots + x_s^2 \tag{1}$$

in integers x_i. Clearly, $r_s(0) = 1$.

Exact formulas for $r_s(n)$ are known for various small s. These include

$$r_2(n) = 4 \sum_{2\ell+1|n} (-1)^\ell, \tag{2}$$

$$r_4(n) = 8 \cdot 3^\delta \sum_{2\ell+1|n} (2\ell+1), \text{ where } \delta = \begin{cases} 1 & \text{if } n \text{ is even,} \\ 0 & \text{otherwise,} \end{cases} \tag{3}$$

$$r_8(n) = 16 \sum_{d|n} (-1)^{n+d} d^3. \tag{4}$$

The formulas (2), (3) and (4) are derived by equating the coefficients in well known identities of Jacobi. See, for example, page 307 of Smith [3], or Chapter IX of Hardy [2], or page 121 of Grosswald [1].

Email address: `ssw@cerias.purdue.edu` (Samuel S. Wagstaff, Jr.).

Similar formulas are known for even s up to about 24. Formulas for odd $s > 1$ are more complicated. They may involve class numbers and, when $s > 8$, coefficients of cusp forms.

In this note we prove congruences for $r_s(n)$ modulo $2s$ for infinitely many s. It is clear from (2), (3) and (4) that for all $n \geq 1$ we have

$$4|r_2(n), \qquad 8|r_4(n), \qquad 16|r_8(n).$$

In other words, $r_s(n) \equiv 0 \pmod{2s}$ for $s = 2, 4, 8$, and for all $n \geq 1$. This congruence also holds for $s = 1$.

However, it is not true that $r_s(n) \equiv 0 \pmod{2s}$ for all s and $n \geq 1$. For example, $r_3(27) = 32 \equiv 2 \pmod{6}$, $r_5(20) = 752 \equiv 2 \pmod{10}$, $r_6(3) = 160 \equiv 4 \pmod{12}$ and $r_9(6) = 7932 \equiv 12 \pmod{18}$. The following theorems explain these values.

Theorem 1 *Let p be a prime and k and n be positive integers. Let $s = p^k$. If $p = 2$, then $r_s(n) \equiv 0 \pmod{2s}$. If p is odd, then*

$$r_s(n) \equiv \begin{cases} 2 \pmod{2p} & \text{if } n = st^2 \text{ for some positive integer } t, \\ 0 \pmod{2p} & \text{otherwise.} \end{cases}$$

Proof. Suppose first that $p = 2$ and $s = 2^k$. We prove by induction on k that $r_s(n) \equiv 0 \pmod{2s}$. Formulas (2), (3) and (4) give the result for $k = 1$, 2 and 3.

If we let

$$\vartheta(q) = \sum_{n=-\infty}^{\infty} q^{n^2} = 1 + 2\sum_{n=1}^{\infty} q^{n^2}$$

denote the the generating function of the squares, then it is well known that

$$(\vartheta(q))^s = 1 + \sum_{n=1}^{\infty} r_s(n)q^n = \sum_{n=0}^{\infty} r_s(n)q^n$$

is the generating function for $r_s(n)$. Now $(\vartheta(q))^{2s} = ((\vartheta(q))^s)^2$, so for $n \geq 0$,

$$\sum_{n=0}^{\infty} r_{2s}(n)q^n = \left(\sum_{i=0}^{\infty} r_s(i)q^i\right)^2.$$

When we equate the coefficients of q^n on each side we find, for $n \geq 0$,

$$r_{2s}(n) = \sum_{i=0}^{n} r_s(i) r_s(n-i). \tag{5}$$

Assume by induction that $r_s(n) \equiv 0 \pmod{2s}$ for a given s and all $n > 0$. Then Equation (5) implies that $r_{2s}(n) \equiv 2r_s(0)r_s(n) \pmod{4s^2}$. Using $s \geq 2$, $r_s(0) = 1$ and the inductive hypothesis again, we find $r_{2s}(n) \equiv 0 \pmod{4s}$, and the proof is complete for $p = 2$.

Now suppose that p is an odd prime and $s = p^k$ with $k \geq 1$. If the s-tuple $(x_1, \ldots, x_s)$ is a solution to (1) counted in $r_s(n)$, then at least one $x_i \neq 0$. Let x_j be the first nonzero one. Then the pairing

$$(x_1, \ldots, x_j, \ldots, x_s) \longleftrightarrow (x_1, \ldots, -x_j, \ldots, x_s)$$

pairs distinct solutions to (1) and shows that their number is even, that is, $r_s(n) \equiv 0 \pmod{2}$. (In fact, this pairing shows that $r_s(n)$ is even for any positive integers s and n.)

Let σ denote the permutation of the s-tuple $(x_1, \ldots, x_s)$ that rotates the components one position to the left. Let G be the permutation group generated by σ. Clearly, G is cyclic of order s. When $(x_1, \ldots, x_s)$ is a solution to (1) so is every permutation of this s-tuple. The $r_s(n)$ solutions to (1) are partitioned by the action of G into disjoint orbits. The size of the orbit of $(x_1, \ldots, x_s)$ under the action of G divides the order of G, and hence is a power of p. The size is 1 if and only if $x_i = t$ for $i = 1, \ldots, s$ and some t. If $n = st^2$, then the orbits of the two s-tuples $(t, t, \ldots, t)$ and $(-t, -t, \ldots, -t)$ each have size 1. In all other cases the size of the orbit is a multiple of p. Therefore, the number of solutions to (1) is a multiple of p when n does not have the form st^2, and it is 2 more than a multiple of p when $n = st^2$ for some positive integer t. This completes the proof.

Corollary 2 *If s is an odd prime and n is a positive integer, then*

$$r_s(n) \equiv \begin{cases} 2 \pmod{2s} & \text{if } n = st^2 \text{ for some positive integer } t, \\ 0 \pmod{2s} & \text{otherwise.} \end{cases}$$

Theorem 3 *If $s = 2^k m > 0$, with m odd and $k \geq 0$, then for all $n > 0$ we have*

$$r_s(n) \equiv 0 \pmod{2^{k+1}}.$$

Proof. If $m = 1$, this theorem is just the first part of Theorem 1. Therefore, we may assume $m \geq 3$.

Use induction on k. As noted in the proof of Theorem 1, $r_s(n)$ is even for any positive integers s and n. This shows the base step $k = 0$. Assume the congruence holds for some k and some m, that is, for some s. We prove it for $k+1$ and the same m, that is, for $2s$. The convolution (5) applies and shows that $r_{2s}(n) \equiv 2r_s(n) \pmod{2^{2(k+1)}}$. Since $2(k+1) \geq k+2$ and 2^{k+1} divides $r_s(n)$, we have $r_{2s}(n) \equiv 0 \pmod{2^{k+2}}$, and the proof is complete.

Remark. Tables of $r_s(n)$ suggest that Theorems 1 and 3 describe *all* congruences modulo a divisor of $2s$ satisfied by $r_s(n)$ for all $n > 0$. For example, when $s = 9$, $r_9(n) \equiv 0, 2, 6, 8, 12, 14 \pmod{18}$ for $n = 1, 225, 3, 9, 6, 81$, respectively. Likewise, $r_{15}(n) \equiv 0, 2, 4, \ldots, 28 \pmod{30}$ when $n = 1, 540, 120, 5, 60, 3, 10, 30, 330, 70, 9, 135, 25, 90, 15$, respectively. Also, $r_{18}(n) \equiv 0, 4, 8, \ldots, 32 \pmod{36}$ for $n = 1, 18, 180, 3, 9, 45, 6, 36, 90$, respectively. In each of these examples, the value of n is the smallest one for which $r_s(n)$ lies in the specified congruence class.

Acknowledgements. The author thanks the Center for Education and Research in Information Assurance and Security at Purdue University for support while this work was done.

References

[1] E. Grosswald. *Representations of Integers as Sums of Squares*. Springer-Verlag, New York, New York, 1985.

[2] G. H. Hardy. *Ramanujan; Twelve Lectures on Subjects Suggested by his Life and Work*. Cambridge Univ. Press, Cambridge, 1940.

[3] H. J. S. Smith. *Report on the Theory of Numbers*. Reprinted by Chelsea, New York, 1965.