Bull. Aust. Math. Soc. **94** (2016), 167–168
doi:10.1017/S0004972716000083

TOPICS IN DIVISIBILITY: PAIRWISE COPRIMALITY, THE GCD OF SHIFTED SETS AND POLYNOMIAL IRREDUCIBILITY

RANDELL HEYMAN

(Received 15 December 2015; first published online 2 January 2016)

2010 *Mathematics subject classification*: primary 11A05; secondary 11C08, 11R09.

Keywords and phrases: divisibility, pairwise coprimality, polynomial irreducibility, greatest common divisor of sets.

By 3000 BC, there is evidence of the use of divisibility in Egypt and Mesopotamia (see for example [7]). Divisibility naturally led to the concepts of primality, common divisors and, eventually, polynomial irreducibility. In this thesis, we explore some modern results regarding these three concepts.

In the first chapter we explore pairwise coprimality and pairwise noncoprimality. Given a subset A of the set $\{1, \dots, k\}^2$, we say that $(a_1, \dots, a_k) \in \mathbb{Z}^k$ exhibits *pairwise coprimality over* A if $\gcd(a_i, a_j) = 1$ for all $(i, j) \in A$. When the set A is obvious, we might just say that $(a_1, \dots, a_k)$ exhibits *pairwise coprimality*. We say that $(a_1, \dots, a_k)$ is *totally pairwise coprime* if $\gcd(a_i, a_j) = 1$ for all $1 \le i < j \le k$. We say that $(a_1, \dots, a_k)$ is *pairwise noncoprime* if $\gcd(a_i, a_j) \ne 1$ for all $1 \le i < j \le k$. Pairwise coprimality has a long history. It is a requirement of the Chinese remainder theorem, whose proof has been known for at least 750 years (see [7, pages 131–132]). The Chinese remainder theorem is important in many areas of modern-day mathematics. Some applications in modular multiplication, bridging computations, coding theory and cryptography can be found in [3, pages 33–184] and some comments regarding modular multiplication applications can be found in [8, pages 287–290]. To date, pairwise coprimality calculations have also been necessary for quantifying k-tuples that are pairwise noncoprime (see [5, 6] and [10] and further comments by T. Freiberg [unpublished manuscript].

We give pairwise coprimality results for triples and show that the methods are not generally suitable for larger tuples. We then use more advanced techniques to give general results for larger tuples. This leads to results for tuples of polynomials over finite fields that exhibit pairwise coprimality. We finish the chapter with a

Thesis submitted to the University of New South Wales in July 2015; degree approved on 25 September 2015; supervisor Igor Shparlinski.

brief discussion regarding tuples that exhibit both pairwise coprime and pairwise noncoprime conditions.

In the second chapter we study the greatest common divisor of shifted sets. Our main result is a dual problem to the approximate common divisor problem, which has applications in cryptography. Given a set of k positive integers $\{a_1, \ldots, a_k\}$ and an integer parameter H, we study the greatest common divisor of small additive shifts of its elements by integers h_i with $|h_i| \le H$, $i = 1, \ldots, k$. In particular, we show that for any choice of $a_1, \ldots, a_k$ there are shifts of this type for which the greatest common divisor of $a_1 + h_1, \ldots, a_k + h_k$ is much larger than H. We end with some related results.

In the third chapter we consider integer coefficient polynomial irreducibility. Some of the analysis could be the basis for further results for polynomials with rational coefficients, due to Gauss's lemma [4, Article 42]. It is well known that almost all polynomials in rather general families of $\mathbb{Z}[x]$ are irreducible (see [1, 2, 11] and references therein). There are also known polynomial-time irreducibility tests and polynomial-time factoring algorithms (see for example [9]). However, it is always interesting to study large classes of polynomials that are known to be irreducible.

We quantify the number of polynomials of bounded height that are irreducible by the Eisenstein criterion. Next, we count the number of polynomials of bounded height that are irreducible by the Eisenstein criterion after the additive shift of a variable. Then we consider the Dumas criterion—in this context, a generalisation of the Eisenstein criterion. Our main results in this section are estimates of the number of polynomials of bounded height that are irreducible due to the Dumas criterion. Finally, we give various enumerations of the number of irreducible binomials in finite fields.

References

[1] S. Akiyama and A. Pethő, 'On the distribution of polynomials with bounded roots II. Polynomials with integer coefficients', *Unif. Distrib. Theory* **9**(1) (2014), 5–19.
[2] R. Dietmann, 'On the distribution of Galois groups', *Mathematika* **58** (2012), 35–44.
[3] C. Ding, D. Pei and A. Salomaa, *The Chinese Remainder Theorem* (World Scientific, Singapore, 1996).
[4] C. F. Gauss, *Disquisitiones Arithmeticae*, English edn (Springer, New York, 1986).
[5] R. Heyman, 'Pairwise non-coprimality of triples', Preprint, 2014, arXiv:1309.5578 [math.NT].
[6] J. Hu, 'Pairwise relative primality of positive integers', Preprint, 2014, arXiv:1406.3113 [math.NT].
[7] V. J. Katz, *A History of Mathematics*, brief edn (Pearson/Addison-Wesley, Boston, MA, 2003).
[8] D. E. Knuth, *The Art of Computer Programming, Vol. 2, Seminumerical Algorithms*, 3rd edn (Addison-Wesley, Boston, MA, 1998).
[9] A. K. Lenstra, H. W. Lenstra and L. Lovász, 'Factoring polynomials with rational coefficients', *Math. Ann.* **261** (1982), 515–534.
[10] P. Moree, 'Counting carefree couples', *Math. News.* **24**(4) (2014), 103–110.
[11] D. Zywina, 'Hilbert's irreducibility theorem and the larger sieve', Preprint, 2010, arXiv:1011.6465 [math.NT].

RANDELL HEYMAN, School of Mathematics and Statistics,
University of New South Wales, Sydney, New South Wales 2052, Australia
e-mail: randell@unsw.edu.au

https://doi.org/10.1017/S0004972716000083 Published online by Cambridge University Press