

Dougherty, Steven T.; Park, Young Ho

On modular cyclic codes. (English) Zbl 1130.94333
Finite Fields Appl. 13, No. 1, 31-57 (2007).

Summary: We study cyclic codes of arbitrary length N over the ring of integers modulo M . We first reduce this to the study of cyclic codes of length $N = p^k n$ (n prime to p) over the ring \mathbb{Z}_{p^e} for prime divisors p of N . We then use the discrete Fourier transform to obtain an isomorphism γ between $\mathbb{Z}_{p^e}[X]/(X^N - 1)$ and a direct sum $\bigoplus_{i \in I} \mathcal{S}_i$ of certain local rings which are ambient spaces for codes of length p^k over certain Galois rings, where I is the complete set of representatives of p -cyclotomic cosets modulo n . Via this isomorphism we may obtain all codes over \mathbb{Z}_{p^e} from the ideals of \mathcal{S}_i . The inverse isomorphism of γ is explicitly determined, so that the polynomial representations of the corresponding ideals can be calculated. The general notion of higher torsion codes is defined and the ideals of \mathcal{S}_i are classified in terms of the sequence of their torsion codes.

MSC:

- 94B15 Cyclic codes
- 94B05 Linear codes, general
- 11T71 Algebraic coding theory; cryptography (number-theoretic aspects)
- 14H20 Singularities of curves, local rings

Cited in **2** Reviews
Cited in **23** Documents

Keywords:

cyclic codes; constacyclic codes; Galois rings; discrete Fourier transforms; local rings; torsion codes

Full Text: [DOI](#)

References:

- [1] Abualrub, T.; Oehmke, R., On the generators of \mathbb{Z}_4 cyclic codes of length 2^e , IEEE trans. inform. theory, 49, 9, 2126-2133, (2003) · [Zbl 1283.94126](#)
- [2] Blackford, T., Cyclic codes over \mathbb{Z}_4 of oddly even length, Discrete appl. math., 128, 27-46, (2003) · [Zbl 1040.94013](#)
- [3] Calderbank, A.R.; Sloane, N.J.A., Modular and p -adic cyclic codes, Design codes cryptogr., 6, 21-35, (1995) · [Zbl 0848.94020](#)
- [4] Castagnoli, G.; Massey, J.L.; Schoeller, P.A.; von Seemann, N., On repeated-root cyclic codes, IEEE trans. inform. theory, 37, 2, 337-342, (1991) · [Zbl 0721.94016](#)
- [5] S.T. Dougherty, S. Ling, Cyclic codes over \mathbb{Z}_4 of even length, 2004, in preparation.
- [6] Dougherty, S.T.; Shiromoto, K., MDR codes over \mathbb{Z}_k , IEEE trans. inform. theory, 46, 1, 265-269, (2000) · [Zbl 1001.94039](#)
- [7] Kanwar, P.; López-Permouth, S.R., Cyclic codes over the integers modulo p^m , Finite fields appl., 3, 334-352, (1997) · [Zbl 1055.94541](#)
- [8] S.Y. Kim, Liftings of the ternary Golay code, Master's Thesis, Kangwon National University, 2004.
- [9] van Lint, J.H., Repeated-root cyclic codes, IEEE trans. inform. theory, 37, 2, 343-345, (1991) · [Zbl 0721.94017](#)
- [10] McDonald, B.R., Finite rings with identity, (1974), Dekker New York · [Zbl 0294.16012](#)
- [11] MacWilliams, F.J.; Sloane, N.J.A., The theory of error-correcting codes, (1977), North-Holland Amsterdam · [Zbl 0369.94008](#)
- [12] Pless, V.S.; Qian, Z., Cyclic codes and quadratic residue codes over \mathbb{Z}_4 , IEEE trans. inform. theory, 42, 5, 1594-1600, (1996) · [Zbl 0859.94018](#)

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.