Computations and Observations on Congruence Covering Systems

Andrew Lott

Millsaps College Mathematics

Congruence Classes

For $n, r \in \mathbb{N}$ with $0 \leq r < n$, the congruence class $r \pmod{n}$ is the set of integers which leave a remainder of r when divided by n.

Here, r is the residue and n is the modulus.

Examples:

$$1 \pmod{2} = \{\ldots, -9, -7, -5, -3, -1, 1, 3, 5, 7, 9, \ldots\}$$
$$0 \pmod{3} = \{\ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}$$
$$3 \pmod{4} = \{\ldots, -17, -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\}$$

Congruence Covering Systems

A covering system is a set of congruence classes whose union is $\mathbb{Z}$.

The simplest example is $\{0 \pmod 2, 1 \pmod 2\}$.

Distinct Covering Systems

What if we require the moduli to be distinct? Now the problem becomes more interesting.

With a little bit of effort, you can show that it's impossible to cover $\mathbb{Z}$ with only four congruence classes with distinct moduli.

However, it is possible to cover $\mathbb{Z}$ with 5 distinct moduli:

$$\{0 \pmod 2, 0 \pmod 3, 1 \pmod 4, 1 \pmod 6, 11 \pmod{12}\}.$$

How do we prove it covers $\mathbb{Z}$?

The following lemma allows us to check whether a congruence system covers $\mathbb{Z}$ in a finite number of steps.

Lemma

Let $\{r_1 \pmod{m_1}, \ldots, r_n \pmod{m_n}\}$ *be a system of congruences, and let* $L = LCM(m_1, \ldots, m_n)$*. If the system covers* $\{1, \ldots, L\}$*, then it covers* $\mathbb{Z}$*.*

A computer can do this quickly.

Let's use the lemma to prove

$$\{0 \pmod 2, 0 \pmod 3, 1 \pmod 4, 1 \pmod 6, 11 \pmod{12}\}.$$

is a covering system.

The LCM of the moduli is 12, so we have to check if the system covers $\{1, 2, \ldots, 12\}$.

1	2	3	4	5	6	7	8	9	10	11	12

1	2	3	4	5	6	7	8	9	10	11	12

0 (mod 2)

1	2	3	4	5	6	7	8	9	10	11	12

0 (mod 3)

1	2	3	4	5	6	7	8	9	10	11	12

1 (mod 4)

1	2	3	4	5	6	7	8	9	10	11	12

1 (mod 6)

1	2	3	4	5	6	7	8	9	10	11	12

11 (mod 12)

Thus,

$$\{0 \pmod 2, 0 \pmod 3, 1 \pmod 4, 1 \pmod 6, 11 \pmod{12}\}$$

is a covering system.

Notice it is also minimal. That is, if any congruence class were removed, the system would no longer cover $\mathbb{Z}$.

We can transform a distinct minimal covering system into another distinct minimal covering system in the following ways.

(1) Let $a \in \mathbb{Z}$ and add a to each residue in the covering system.

(2) Let L be the LCM of the moduli. Let u be a unit mod L and multiply each residue by u.

(3) Multiply each residue and each modulus by 2, thus giving a distinct system covering $0 \pmod 2$. Now, include $1 \pmod 2$.

We define equivalence classes of distinct covering systems based on these transformations.

Computational goal: classify all distinct minimal covering systems with at most 10 moduli.

We make heavy use of the lemmas and algorithms in a paper by Jenkin and Simpson.

The following lemma is particularly useful.

Lemma

If $S = \{r_1 (\text{mod } m_1), \ldots, r_k (\text{mod } m_k)\}$ *is a minimal covering system and* $\prod_{i=1}^{t} p_i^{a_i}$ *is the prime factorization of* $\operatorname{lcm}(m_1, \ldots, m_k)$, *then* $\sum_{i=1}^{t} a_i(p_i - 1) + 1 \leq k$.

This reduces our search to finitely many lists of moduli.

k	distinct minimal covering systems with k moduli, up to equivalence
5	$\{[1,2],[1,3],[2,4],[2,6],[0,12]\}$
6	$\{[1,2],[1,3],[2,4],[2,6],[4,8],[0,24]\}$, $\{[1,2],[1,3],[2,4],[4,8],[8,12],[0,24]\}$, $\{[1,2],[1,3],[2,6],[4,8],[6,12],[0,24]\}$
7	15 equivalence classes, 11 sets of moduli: $\{[1,2],[1,3],[2,4],[2,6],[4,8],[8,16],[0,48]\}$, $\{[1,2],[1,3],[2,4],[2,6],[3,9],[6,18],[0,36]\}$, $\{[1,2],[1,3],[2,4],[2,6],[6,9],[12,18],[0,36]\}$, $\{[1,2],[1,3],[2,4],[2,6],[8,16],[12,24],[0,48]\}$, $\{[1,2],[1,3],[2,4],[4,8],[8,12],[8,16],[0,48]\}$, $\{[1,2],[1,3],[2,4],[4,8],[8,16],[8,24],[0,48]\}$, $\{[1,2],[1,3],[2,4],[3,9],[8,12],[6,18],[0,36]\}$, $\{[1,2],[1,3],[2,4],[6,9],[8,12],[12,18],[0,36]\}$, $\{[1,2],[1,3],[2,4],[8,12],[8,16],[12,24],[0,48]\}$, $\{[[1,2],[1,3],[2,6],[4,8],[6,12],[8,16],[0,48]\}$, $\{[1,2],[1,3],[2,6],[3,9],[6,12],[6,18],[0,36]\}$, $\{[1,2],[1,3],[2,6],[6,9],[6,12],[12,18],[0,36]\}$, $\{[1,2],[1,3],[2,6],[6,12],[8,16],[12,24],[0,48]\}$, $\{[1,2],[2,4],[2,6],[3,9],[4,12],[6,18],[0,36]\}$, $\{[1,2],[2,4],[2,6],[6,9],[4,12],[12,18],[0,36]\}$

k	distinct minimal covering systems with k moduli, up to equivalence
8	85 equivalence classes, one or two with each of the following 50 sets of moduli: $\{2,3,4,6,8,9,18,72\}$, $\{2,3,4,6,8,9,36,72\}$, $\{2,3,4,6,8,16,32,96\}$, $\{2,3,4,6,8,18,36,72\}$, $\{2,3,4,6,8,32,48,96\}$, $\{2,3,4,6,9,18,24,72\}$, $\{2,3,4,6,9,24,36,72\}$, $\{2,3,4,6,16,24,32,96\}$, $\{2,3,4,6,18,24,36,72\}$, $\{2,3,4,6,24,32,48,96\}$, $\{2,3,4,8,9,12,18,72\}$, $\{2,3,4,8,9,12,36,72\}$, $\{2,3,4,8,9,18,24,36\}$, $\{2,3,4,8,9,18,24,72\}$, $\{2,3,4,8,9,24,36,72\}$, $\{2,3,4,8,12,16,32,96\}$, $\{2,3,4,8,12,18,36,72\}$, $\{2,3,4,8,12,32,48,96\}$, $\{2,3,4,8,16,24,32,96\}$, $\{2,3,4,8,16,32,48,96\}$, $\{2,3,4,8,18,24,36,72\}$, $\{2,3,4,8,24,32,48,96\}$, $\{2,3,4,9,12,18,24,72\}$, $\{2,3,4,9,12,24,36,72\}$, $\{2,3,4,12,16,24,32,96\}$, $\{2,3,4,12,18,24,36,72\}$, $\{2,3,4,12,24,32,48,96\}$, $\{2,3,6,8,9,12,18,72\}$, $\{2,3,6,8,9,12,36,72\}$, $\{2,3,6,8,9,18,24,36\}$, $\{2,3,6,8,9,18,36,72\}$, $\{2,3,6,8,12,16,32,96\}$, $\{2,3,6,8,12,18,36,72\}$, $\{2,3,6,8,12,32,48,96\}$, $\{2,3,6,9,12,18,24,72\}$, $\{2,3,6,9,12,24,36,72\}$, $\{2,3,6,9,18,24,36,72\}$, $\{2,3,6,12,16,24,32,96\}$, $\{2,3,6,12,18,24,36,72\}$, $\{2,3,6,12,24,32,48,96\}$, $\{2,4,6,8,9,12,18,72\}$, $\{2,4,6,8,9,12,36,72\}$, $\{2,4,6,8,9,18,24,36\}$, $\{2,4,6,8,9,18,24,72\}$, $\{2,4,6,8,9,24,36,72\}$, $\{2,4,6,9,12,18,24,72\}$, $\{2,4,6,9,12,24,36,72\}$, $\{2,4,8,9,12,18,24,36\}$, $\{2,4,8,9,12,18,24,72\}$, $\{2,4,8,9,12,24,36,72\}$

k	distinct minimal covering systems with k moduli, up to equivalence
9	585 equivalence classes, 248 sets of moduli: • $1, 2, 4$ or 6 equivalence classes for each set of moduli • All systems have minimum modulus 2 • Maximum moduli: $30, 48, 60, 72, 80, 108, 144, 192$ • Moduli have no prime factors greater than 5
10	6267 equivalence classes, 1652 sets of moduli • $1, 2, 4, 6, 8, 12$, or 18 equivalence classes for each set of moduli • All systems have minimum modulus 2 • Maximum moduli: $30, 40, 45, 48, 60, 72, 80, 90, 96, 108, 120, 144, 160, 192, 216, 288, 384$ • Moduli have no prime factors greater than 5

Notice that every system listed uses the modulus 2. Erdős conjectured that

$$\{[0,3],\ [0,4],\ [0,5],\ [1,6],\ [6,8],\ [3,10],\ [2,12],\ [11,15],\ [7,20],\ [10,24],\ [2,30],\ [34,40],\ [59,60],\ [98,120]\}$$

is the smallest possible distinct covering system with minimum modulus greater than or equal to 3. There are 14 moduli in this system.

Erdős was wrong. We found a distinct minimal covering system with 12 moduli with minimum modulus 3:

$$\{[0,3],\ [0,4],\ [1,6],\ [5,8],\ [2,9],\ [2,12],\ [6,16],\ [17,18],\ [10,24],\ [23,36],\ [46,48],\ [41,72]\}.$$

We perfomed computations to show this is the smallest system with minimum modulus greater than or equal to 3.

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132
133	134	135	136	137	138	139	140	141	142	143	144

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132
133	134	135	136	137	138	139	140	141	142	143	144

$0 \pmod 3$

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132
133	134	135	136	137	138	139	140	141	142	143	144

$0 \pmod 4$

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132
133	134	135	136	137	138	139	140	141	142	143	144

$1 \pmod 6$

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132
133	134	135	136	137	138	139	140	141	142	143	144

$5 \pmod{8}$

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132
133	134	135	136	137	138	139	140	141	142	143	144

$2 \pmod 9$

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132
133	134	135	136	137	138	139	140	141	142	143	144

$2 \pmod{12}$

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132
133	134	135	136	137	138	139	140	141	142	143	144

$6 \pmod{16}$

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132
133	134	135	136	137	138	139	140	141	142	143	144

$17 \pmod{18}$

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132
133	134	135	136	137	138	139	140	141	142	143	144

$10 \pmod{24}$

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132
133	134	135	136	137	138	139	140	141	142	143	144

$23 \pmod{36}$

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132
133	134	135	136	137	138	139	140	141	142	143	144

$46 \pmod{48}$

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132
133	134	135	136	137	138	139	140	141	142	143	144

$41 \pmod{72}$

Acknowledgments

This research took place during the Summer 2022 Kinnaird Institute Research Experience at Millsaps College led by Alex Rice. The other group members were Prarthana Bhatia, Raj Agrawal, Powers Lamb, Christine Rose Ward, Kratik Gupta.