

**XXVIII**  
**Межрегиональная олимпиада**  
**школьников им. И.Я.Верченко по математике и**  
**криптографии**

**УСЛОВИЯ И РЕШЕНИЯ**



Москва 2019

## 11 КЛАСС

### УСЛОВИЯ ЗАДАЧ

1. Для зашифрования слова из пяти букв каждая его буква заменяется на число согласно таблице. Полученный набор чисел  $(x_0, x_1, x_2, x_3, x_4)$  затем преобразуется в набор  $(y_0, y_1, y_2, y_3, y_4)$  по следующему правилу. Сначала вычисляют вспомогательные числа  $y'_0, y'_1, y'_2, y'_3, y'_4$  по формулам

$$y'_0 = 2^0 \cdot x_0 + 2^4 \cdot x_1 + 2^3 \cdot x_2 + 2^2 \cdot x_3 + 2^1 \cdot x_4,$$

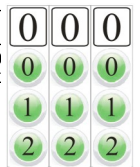
$$y'_k = (2^k \cdot x_0 + 2^{k-1} \cdot x_1 + \dots + 2^0 \cdot x_k) + (2^4 \cdot x_{k+1} + 2^3 \cdot x_{k+2} + \dots + 2^{k+1} \cdot x_4), k=1,2,3.$$

$$y'_4 = 2^4 \cdot x_0 + 2^3 \cdot x_1 + 2^2 \cdot x_2 + 2^1 \cdot x_3 + 2^0 \cdot x_4.$$

А затем полагают  $y_k$  равным остатку от деления числа  $y'_k$  на 32. Расшифруйте исходное слово, если  $(y_0, y_1, y_2, y_3, y_4) = (11, 27, 2, 16, 0)$ .

					Ё																																		0	0	0																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																															
0	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	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	522	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545	546	547	548	549	550	551	552	553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571	572	573	574	575	576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593	594	595	596	597	598	599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623	624	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	649	650	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675	676	677	678	679	680	681	682	683	684	685	686	687	688	689	690	691	692	693	694	695	696	697	698	699	700	701	702	703	704	705	706	707	708	709	710	711	712	713	714	715	716	717	718	719	720	721	722	723	724	725	726	727	728	729	730	731	732	733	734	735	736	737	738	739	740	741	742	743	744	745	746	747	748	749	750	751	752	753	754	755	756	757	758	759	760	761	762	763	764	765	766	767	768	769	770	771	772	773	774	775	776	777	778	779	780	781	782	783	784	785	786	787	788	789	790	791	792	793	794	795	796	797	798	799	800	801	802	803	804	805	806	807	808	809	810	811	812	813	814	815	816	817	818	819	820	821	822	823	824	825	826	827	828	829	830	831	832	833	834	835	836	837	838	839	840	841	842	843	844	845	846	847	848	849	850	851	852	853	854	855	856	857	858	859	860	861	862	863	864	865	866	867	868	869	870	871	872	873	874	875	876	877	878	879	880	881	882	883	884	885	886	887	888	889	890	891	892	893	894	895	896	897	898	899	900	901	902	903	904	905	906	907	908	909	910	911	912	913	914	915	916	917	918	919	920	921	922	923	924	925	926	927	928	929	930	931	932	933	934	935	936	937	938	939	940	941	942	943	944	945	946	947	948	949	950	951	952	953	954	955	956	957	958	959	960	961	962	963	964	965	966	967	968	969	970	971	972	973	974	975	976	977	978	979	980	981	982	983	984	985	986	987	988	989	990	991	992	993	994	995	996	997	998	999	1000

2. При входе в личный кабинет на терминале требуется ввести трехзначный пароль  $x_1, x_2, x_3$ , где  $x_i \in \{0, 1, 2\}$ . Для этого на терминале имеются 3 окошка, а под каждым окошком расположены три кнопки. При нажатии на кнопку в окошке над ней появляется соответствующая цифра. Сейчас в окошках выставлена комбинация 000. Какое наименьшее количество нажатий кнопок потребуется, чтобы перебрать все возможные варианты пароля?



3. В Крипто-Вегасе на табло игрового автомата отображаются два натуральных числа  $x_0=5$  и  $y_0=201$ . При нажатии кнопки первое из этих чисел заменяется на  $x_1=r_{11}(a \cdot x_0+b)$ , где  $a$  и  $b$  – некоторые неизвестные натуральные числа, а второе число заменяется на  $y_1=r_{2017}(y_0+523)$ . Здесь  $r_k(m)$  – остаток от деления натурального числа  $m$  на  $k$ . Нажав кнопку еще раз, получим (по таким же формулам) числа  $x_2=r_{11}(a \cdot x_1+b)$  и  $y_2=r_{2017}(y_1+523)$  и так далее. Игрок получает приз, если при очередном нажатии на табло загорятся числа  $x_n=4$  и  $y_n=1993$ . Определите

а) какие из следующих четырех последовательностей **(1)**: (2, 5, 4, 7, 1), **(2)**: (6, 9, 7, 1, 3), **(3)**: (7, 10, 9, 2, 8), **(4)**: (1, 0, 8, 8, 7) при надлежащем выборе  $a$  и  $b$  и вышеуказанных фиксированных  $x_0, y_0$  могли бы совпасть с последовательностью  $(x_1, \dots, x_5)$ , полученной на этом игровом автомате? б) может ли игрок получить приз, если  $(x_1, \dots, x_5)$  – одна из (реализуемых) последовательностей из пункта а)?

4. Для подтверждения переводимой в банк суммы братья **А** и **В** используют «кольцевую подпись», которая не позволяет определить, кто именно из них совершил перевод. **А** имеет свой открытый ключ  $e_A=5$  и некий секрет, позволяющий для любого натурального  $u$  ( $u \leq 90$ ) находить  $x_A$  такое, что  $u=r_{91}(x_A^{e_A})$ . Здесь  $r_k(m)$  – остаток от деления натурального числа  $m$  на  $k$ . (**У В** есть свой ключ  $e_B=25$  и свой секрет.) Тогда **А** для подписи суммы  $M$  случайно выбирает натуральные числа  $x_B$  и  $v$ , не превосходящие 100, вычисляет  $y_B=r_{91}(x_B^{e_B})$  и находит  $u_A$  из уравнения:

$$r_{101}(M(y_A + M(y_B + v)) - v^3) = 0. (\dot{u})$$

Используя свой секрет, А находит  $x_A$  такой, что  $y_A = r_{91}(x_A^{e_A})$ . Тогда тройка чисел  $(x_A, x_B, v)$  будет подтверждением факта перевода суммы  $M$ . В банке корректность подтверждения проверяют подстановкой  $y_A = r_{91}(x_A^{e_A})$ ,  $y_B = r_{91}(x_B^{e_B})$  и  $v$  в уравнение (i). Например,  $(1, 90, 46)$  корректное подтверждение суммы 46. Постройте хотя бы одно корректное подтверждение суммы  $M=69$ .

5. В некоторые клетки доски  $4 \times 4$  Аня положила по несколько зерен и передала доску Боре (см. рис.). Трансверсалью доски называется набор из 4 клеток, любые две из которых расположены в разных строках и разных столбцах. Боря за один ход может снять одинаковое количество зерен с каждой клетки какой-либо одной трансверсали. За какое минимальное число ходов Боря может снять все зерна с доски?
6. Известно, что оба числа  $p$  и  $p^{2018} + 800$  простые. Докажите, что число  $p^4 + 8$  тоже простое.

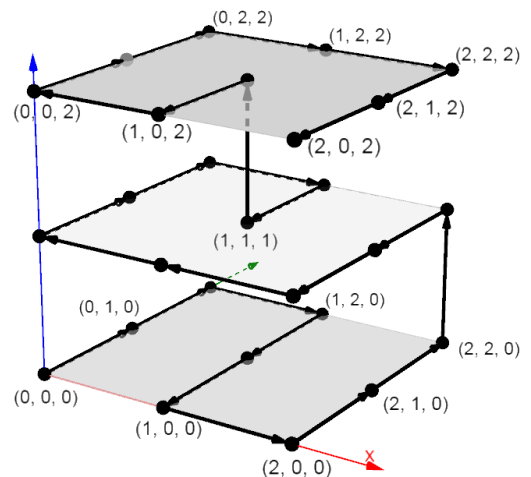
4	5	6	0
5	0	4	6
5	5	3	2
1	5	2	7

## РЕШЕНИЯ ЗАДАЧ

### Задача 1

Заметим, что для  $k=0,1,2,3$  справедливо равенство  $2y'_k - y'_{k+1} = 31x_{k+1}$ . Кроме того  $2y'_4 - y'_0 = 31x_0$ . Числа 31 и (-1) при делении на 32 дают один и тот же остаток 31, то есть  $31 = r_{32}(31) = r_{32}(-1)$ . (Здесь традиционно  $r_{32}(x)$  – остаток от деления числа  $x$  на 32.) Значит  $r_{32}(31x_{k+1}) = r_{32}(-x_{k+1})$  и  $r_{32}(31x_0) = r_{32}(-x_0)$ . В результате получаем формулы, непосредственно выражающие искомые числа  $x_0, x_1, x_2, x_3, x_4$  через данные в условии

$$y_0, y_1, y_2, y_3, y_4$$



$$r_{32}(2y'_k - y'_{k+1}) = r_{32}(31x_{k+1}) = r_{32}(-x_{k+1}) \Rightarrow x_{k+1} = r_{32}(y'_{k+1} - 2y'_k) = r_{32}(y_{k+1} - 2y_k),$$

$$x_0 = r_{32}(y'_0 - 2y'_4) = r_{32}(y_0 - 2y_4).$$

Отсюда находим  $(x_0, x_1, x_2, x_3, x_4) = (11, 5, 12, 12, 0)$ . Зашифрованное слово – ЛЕММА.

Ответ: ЛЕММА.

### Задача 2

Всего имеется  $27 = 3^3$  трехзначных паролей (наборов) из 0, 1 и 2. Один такой пароль 000 уже набран, значит нам остается перебрать оставшиеся 26 вариантов, для чего потребуется по крайней мере 26 нажатий кнопок. Покажем, что 26 нажатий действительно хватит. Для этого все трехзначные наборы упорядочим так, чтобы соседние наборы отличались только в одном символе (классический код Грея). Тогда переход от одного набора к соседнему будет осуществляться нажатием одной кнопки, и всего потребуется как раз 26 нажатий.

Упорядочить так наборы можно многими способами. Одна из возможных идей состоит в следующем: каждый пароль будем интерпретировать как координаты точки в трехмерном пространстве (рис.). Координаты точек, лежащих на прямой, параллельной одной из координатных осей, как раз отличаются только в одном символе. Значит, если, двигаясь параллельно осям, мы обойдем все точки, то тем самым получим требуемое упорядочение. Один из возможных обходов представлен на рисунке.

**Ответ:** 26 нажатий. Один из способов перебора представлен на рисунке:  $(0,0,0)$ ,  $(0,1,0)$ , ...,  $(2,0,2)$ .

### Задача 3

Последовательность  $(x_n)$  задается рекуррентной формулой  $x_n = r_{11}(a \cdot x_{n-1} + b)$ ,  $n \in N$ . (1) Следовательно, значение каждого члена последовательности  $x_n$  (начиная со второго) однозначно вычисляется по значению ее предыдущего члена  $x_{n-1}$ . Покажем, что последовательность (1) получена быть не могла. В ней  $x_0 = 5$  и  $x_1 = 2$ . Значит сразу после 5 всегда должна идти 2, но далее мы видим, что вслед за 5 идет 4. По этой же причине отбраковываем и последовательность (4): после 8 встречается и 7, и 8.

Рассмотрим последовательность (2). Для членов  $x_1$  и  $x_2$  этой последовательности, согласно (1), можем записать:  $x_1 = 6 = r_{11}(a \cdot 5 + b)$ ,  $x_2 = 9 = r_{11}(a \cdot 6 + b)$ . Вычтя из второго равенства первое, найдем  $a = 3$ . Тогда  $b = 2$ . Проверяем далее:  $x_3 = 7 = r_{11}(3 \cdot 9 + 2)$  – верно,  $x_4 = 1 = r_{11}(3 \cdot 7 + 2)$  – верно,  $x_5 = 3 = r_{11}(3 \cdot 1 + 2)$  – неверно. Значит последовательность (2) также отбрасываем.

Рассмотрим последовательность (3). Как и для последовательности (2) находим  $a = 7$ ,  $b = 5$ , а затем убеждаемся, что последовательность (3) проверку проходит. Итак, только последовательность (3) из пункта а) могла быть получена на игровом автомате.

Выясним теперь получит ли в этом случае игрок приз. Выпишем больше членов соответствующей последовательности  $(x_n)$ : 5, 7, 10, 9, 2, 8, 6, 3, 4, 0, 5, 7, ... Видно, что это периодическая последовательность с периодом 10, и в ней встречается 4. Докажем, что последовательность  $(y_n)$  также является периодической, и ее период равен 2017. Заметим что эта последовательность, как и последовательность  $(x_n)$ , обладает тем свойством, что каждый ее последующий член однозначно находится по предыдущему. Поэтому для доказательства периодичности достаточно убедиться, что среди членов последовательности встречаются все целые числа от 0 до 2016. То есть, надо доказать, что для любого целого числа  $m$  от 0 до 2016 существует такое  $n \in N$ , что  $y_n = m$ .

Последовательность  $(y_n)$  (являющаяся ничем иным, как арифметической прогрессией на множестве остатков от деления на 2017) может быть задана формулой  $n$ -ого члена:  $y_n = r_{2017}(201 + 523n)$ ,  $n \in N$ .

Далее

$$y_n = m \Leftrightarrow m = r_{2017}(201 + 523n) \Leftrightarrow \text{существует такое целое } t, \text{ что } 201 + 523n = m + 2017t \Leftrightarrow 523n - 2017t = m - 201$$

Числа 523 и 2017 взаимно простые, поэтому данное линейное диофантово уравнение разрешимо в целых числах относительно  $n$  и  $t$  при любом значении  $m$ . Следовательно, любое значение  $m$  от 0 до 2016, и в частности 1993, встретится в последовательности  $(y_n)$ . Остается заметить, что периоды последовательностей  $(x_n)$  и  $(y_n)$  взаимно простые, поэтому рано или поздно при каком-то  $n \in N$  окажутся справедливыми равенства  $x_n = 4$  и  $y_n = 1993$ .

**Ответ:** а) (3), б) да.

### Задача 4

Надо найти такие числа  $x_A, x_B$  и  $v$ , что если по ним вычислить  $y_A = r_{91}(x_A^{e_A})$ ,  $y_B = r_{91}(x_B^{e_B})$ , а затем подставить эти  $y_A, y_B, v$  и  $M = 69$  в (i), то получится верное равенство. Перепишем уравнение (i) в виде:  $r_{101}(M(y_A + M y_B) + v \cdot (M^2 - v^2)) = 0$ .

Последнее равенство заведомо справедливо, если 
$$\begin{cases} r_{101}(y_A + M y_B) = 0 & (1) \\ r_{101}(M^2 - v^2) = 0 & (2) \end{cases}$$

Второму уравнению системы можно удовлетворить, положив  $v = M$ . Уравнение (1) эквивалентно уравнению  $r_{101}(r_{91}(x_A^{e_A})) = r_{101}(-M \cdot r_{91}(x_B^{e_B}))$ .

Возьмем, например,  $x_B = 1$ . Тогда  $r_{101}(r_{91}(x_A^{e_A})) = r_{101}(-M) \Leftrightarrow r_{91}(x_A^{e_A}) = 101 - M \Leftrightarrow r_{91}(x_A^5) = 32$ .  
Значит, годится  $x_A = 2$ .

**Ответ:** Например, (2, 1, 69).

### Задача 5

Заметим, что в последней строке пустых клеток нет. За один ход Боря может освободить от зерен от силы одну клетку этой строки. Следовательно, ему придется сделать *минимум* 4 хода. Более того, в этой строке есть клетка с 7 зёрнами, а в остальных клетках доски зерен меньше. Значит с этой клетки зерна придется снимать минимум дважды. Поэтому за 4 хода Боря не справится. Покажем как снять зерна за 5 ходов (серым отмечены трансверсали, с которых сняли зерна):

4	5	1	0
5	0	4	1
0	5	3	2
1	0	2	7

4	3	1	0
3	0	4	1
0	5	3	0
1	0	0	7

0	3	1	0
3	0	0	1
0	1	3	0
1	0	0	3

0	3	0	0
3	0	0	0
0	0	3	0
0	0	0	3

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

**Ответ:** За 5 ходов.

### Задача 6

Будем перебирать возможные значения простого числа  $p$ . Если  $p=2$ , то число  $p^{2018} + 800$  четное, что противоречит условию. Пусть  $p=3$ . Тогда число  $3^{2018} + 800$  может и оказаться простым. Убедимся, что для любого другого простого  $p$  число  $p^{2018} + 800$  делится на 3. Действительно, если  $p \neq 3$ , то остаток от деления числа  $p$  на 3 равен либо 1, либо 2. Но остаток от деления числа  $p^{2018}$  на 3 в любом случае будет равен 1 (поскольку  $p^{2018} = (p^2)^{1009}$ , а число  $p^2$  всегда дает остаток 1 при делении на 3). Тогда  $p^{2018} + 800$  делится на 3 (так как 800 дает остаток 2 при делении на 3) и не может быть простым. Таким образом,  $p=3$  – единственно возможный вариант. И тогда  $p^4 + 8 = 3^4 + 8 = 89$  – простое число. Утверждение доказано.