NT & Crypto
MAT4930 *2H22*

Quizzes Q

Summer 2016

Number Sets. Expression $k \in \mathbb{N}$ [read as "k is an element of $\mathbb{N}$" or "k in $\mathbb{N}$"] means that k is a natural number; a ***natnum***. Expression $\mathbb{N} \ni k$ [read as "$\mathbb{N}$ ***owns*** k"] is a synonym for $k \in \mathbb{N}$.

$\mathbb{N}$ = natural numbers = $\{0, 1, 2, \dots\}$.

$\mathbb{Z}$ = integers = $\{\dots, -2, -1, 0, 1, \dots\}$. For the set $\{1, 2, 3, \dots\}$ of positive integers, the ***posints***, use $\mathbb{Z}_+$. Use $\mathbb{Z}_-$ for the negative integers, the ***negints***.

$\mathbb{Q}$ = rational numbers = $\{\frac{p}{q} \mid p \in \mathbb{Z} \text{ and } q \in \mathbb{Z}_+\}$. Use $\mathbb{Q}_+$ for the positive rationals and $\mathbb{Q}_-$ for the negative rationals.

$\mathbb{R}$ = reals. The ***posreals*** $\mathbb{R}_+$ and the ***negreals*** $\mathbb{R}_-$.

$\mathbb{C}$ = complex numbers, also called the ***complexes***.

For $\omega \in \mathbb{C}$, let "$\omega > 5$" mean "ω *is* ***real*** *and* $\omega > 5$". [Use the same convention for $\geq, <, \leq$, and also if 5 is replaced by any real number.]

Use $\overline{\mathbb{R}} = [-\infty, +\infty] := \{-\infty\} \cup \mathbb{R} \cup \{+\infty\}$, the ***extended reals***.

An "***interval of integers***" $[b \,..\, c)$ means the intersection $[b, c) \cap \mathbb{Z}$; ditto for open and closed intervals. So $[\mathrm{e} \,..\, 2\pi] = \{3, 4, 5, 6\} = [3 \,..\, 6] = (2 \,..\, 6]$. We allow b and c to be $\pm\infty$; so $(-\infty \,..\, -1]$ is $\mathbb{Z}_-$. And $[-\infty \,..\, -1]$, is $\{-\infty\} \cup \mathbb{Z}_-$.

Floor function: $\lfloor \pi \rfloor = 3$, $\lfloor -\pi \rfloor = -4$. Ceiling fnc: $\lceil \pi \rceil = 4$. Absolute value: $|-6| = 6 = |6|$ and $|-5 + 2\mathbf{i}| = \sqrt{29}$.

Mathematical objects. Seq: '*sequence*'. poly(s): '*polynomial(s)*'. irred: '*irreducible*'. Coeff: '*coefficient*' and var(s): '*variable(s)*' and parm(s): '*parameter(s)*'. Expr.: '*expression*'. Fnc: '*function*' (so ratfnc: means rational function, a ratio of polynomials). trnfn: '*transformation*'. cty: '*continuity*'. cts: '*continuous*'. diff'able: '*differentiable*'. CoV: '*Change-of-Variable*'. CoI: '*Constant of Integration*'. LoI: '*Limit(s) of Integration*'. RoC: '*Radius of Convergence*'.

Soln: '*Solution*'. Thm: '*Theorem*'. Prop'n: '*Proposition*'. CEX: '*Counterexample*'. eqn: '*equation*'. RhS: '*RightHand side*' of an eqn or inequality. LhS: '*lefthand side*'. Sqrt **or** Sqroot: '*square-root*', e.g, "the sqroot of 16 is 4". Ptn: '*partition*', *but* pt: '*point*' as in "a fixed-pt of a map".

FTC: '*Fund. Thm of Calculus*'. IVT: '*intermediate-Value Thm*'. MVT: '*Mean-Value Thm*'.

The ***logarithm*** function, defined for $x>0$, is $\log(x) := \int_1^x \frac{dv}{v}$. Its inverse-fnc is $\exp()$.

For $x>0$, then, $\exp(\log(x)) = x = \mathrm{e}^{\log(x)}$. For real t, naturally, $\log(\exp(t)) = t = \log(\mathrm{e}^t)$.

PolyExp: '*Polynomial-times-exponential*', e.g, $[3 + t^2]\cdot\mathrm{e}^{4t}$. PolyExp-sum: '*Sum of polyexps*'. E.g, $f(t) := 3t\mathrm{e}^{2t} + [t^2]\cdot\mathrm{e}^t$ is a polyexp-sum.

Phrases. WLOG: '*Without loss of generality*'. IFF: '*if and only if*'. TFAE: '*The following are equivalent*'. ITOf: '*In Terms Of*'. OTForm: '*of the form*'. FTSOC: '*For the sake of contradiction*'. And ⯳ ="Contradiction".

IST: '*It Suffices To*', as in ISTShow, ISTExhibit.

Use w.r.t: '*with respect to*' and s.t: '*such that*'.

Latin: e.g: *exempli gratia*, '*for example*'. i.e: *id est*, '*that is*'. N.B: *Nota bene*, '*Note well*'. inter alia: '*among other things*'. QED: *quod erat demonstrandum*, meaning "end of proof".

Plex [2023g] quizzes so far...

Q1: Fri. 20 Jan Euler $\varphi(56) =$ ⌞.....⌟.

Soln. Note $56 = 2^3 \cdot 7$. As φ is multiplicative,

$$\varphi(56) = \varphi(2^3) \cdot \varphi(7) = 2^2 \cdot [2-1] \cdot [7-1] = 24. \blacklozenge$$

Mod K:=51, the reciprocal $\left\langle \frac{1}{20} \right\rangle_K =$ ⌞ 23 ⌟ $\in [0\,..\,K)$.

[*Hint:* ↯] So $x =$ ⌞ 18 ⌟ $\in [0\,..\,K)$ solves $5 - 20x \equiv_K 2$.

Recipe for Reciprocal: We do *not* need to compute the s-column, but I'll show it for reference.

```
(lightning 51 20)

  n:   r_n   q_n   s_n   t_n
/---------------------------\
  0:    51    --     1     0
  1:    20     2     0     1
  2:    11     1     1    -2
  3:     9     1    -1     3
  4:     2     4     2    -5
  5:     1     2    -9    23
  6:     0 Infty    20   -51
\---------------------------/

  Note    GCD  =  r0 * S  +  r1 * T,  i.e
            1  =  [51]*[-9] + [20]*[23].
```

So $R := \langle 1 \div 20 \rangle_K \equiv_K 23$.

The congruence gives $20x \equiv_K 5 - 2 = 3$. Thus

$$x \equiv_K 23 \cdot [20 \cdot x] \equiv_K 23 \cdot 3 = 69 \equiv_K 18. \blacklozenge$$

Q2: Wed. 25 Jan With $N := 85$, then $\varphi(N) =$ 64. Thus EFT (Euler-Fermat) says that $3^{645} \equiv_N$ 73 $\in [0\,..\,N)$.

φ-fi-foo-fum. Our $\varphi(N) = \varphi(5) \cdot \varphi(17) = 4 \cdot 16 = 64$, as prime-power factoring gives $85 = 5 \cdot 17$. And $645 \equiv_{64} 5$. *Since* $3 \perp 85$, EFT applies, asserting $3^{645} \equiv_{85} 3^5$. I.e,

```
% (mod 645 64)  ->  5

% (repeated-squaring 3 5 85 :symmod nil)

 /--------------------- Mod 85 ----\
  n:      2^n |     Accum |   3^[2^n]
---+----------+-----------+-------------
  0:        1 |         1 |         3 <<
  1:        2 |         3 |         9
  2:        4 |         3 |        81 <<
All:     done |        73 |
 \--------------------- Mod 85 ----/

  So  3^5  is mod-85 congruent to the
product of the << marked values, which is 73,
```

since $81 \cdot 3 \equiv_{85} -4 \cdot 3 = -12 \equiv_{85} 73$. ♦

Alternatively: *We can avoid* Euler-Fermat, *as follows*:

```
%  (repeated-squaring 3 645 85)

 /--------------------- Mod 85 ----\
  n:      2^n |     Accum |   3^[2^n]
---+----------+-----------+-------------
  0:        1 |         1 |         3 <<
  1:        2 |         3 |         9
  2:        4 |         3 |        81 <<
  3:        8 |        73 |        16
  4:       16 |        73 |         1
  5:       32 |        73 |         1
  6:       64 |        73 |         1
  7:      128 |        73 |         1 <<
  8:      256 |        73 |         1
  9:      512 |        73 |         1 <<
All:     done |        73 |
 \--------------------- Mod 85 ----/

  So  3^{645}  is mod-85 congruent to the
product of the << marked values, which is 73.
```

The table shows that $3^{[2^4]} \equiv_{85} 1$. As repeated-squaring of 1 yields 1, the table is constant-1 from then on. ♦

Q3: Fri. 27 Jan Note that $\text{GCD}(55,33,15)=1$. Find particular integers S,T,U so that $55S+33T+15U=1$:

$S=$ 4 , $T=$ -8 , $U=$ 3 .

[*Hint:* $\text{GCD}\big(\text{GCD}(55,33),15\big)=1$.]

Soln. Among the ∞ly many correct triples are $(7,-8,-8)$, $(4,-8,3)$, $(1,-3,3)$, $(-2,2,3)$ and $(-23,7,69)$.

LBolting,

```
(lightning 55 33)

  n:   r_n   q_n   s_n   t_n
/--------------------------\
  0:    55    --     1     0
  1:    33     1     0     1
  2:    22     1     1    -1
  3:    11     2    -1     2
  4:     0 Infty     3    -5
\--------------------------/

  Rename r3,s3,t3  to  GCD,S,T.

  Note    GCD  =  r0 * S  +  r1 * T,  i.e
           11  =  [55]*[-1] + [33]*[2].
```

And, we now want `(lightning 11 15)` but I'll reverse the order to make the table one row shorter.

```
(lightning 15 11)

  n:   r_n   q_n   s_n   t_n
/--------------------------\
  0:    15    --     1     0
  1:    11     1     0     1
  2:     4     2     1    -1
  3:     3     1    -2     3
  4:     1     3     3    -4
  5:     0 Infty   -11    15
\--------------------------/
```

So $1 = 11\cdot[-4] + 15\cdot 3$. Substituting from the 1st LBolt,

$$\begin{aligned} 1 &= \big[55\cdot[-1] + 33\cdot 2\big]\cdot[-4] + 15\cdot 3 \\ &= 55\cdot 4 + 33\cdot[-8] + 15\cdot 3\,. \end{aligned}$$ ♦

Exploration. Since $\text{GCD}(55,33)=11$, the 1-parameter family of Bézout-pairs for $(55,33)$ is

$$\begin{aligned} 11 &= \big[-1 + \tfrac{33}{11}\cdot n\big]\cdot 55 + \big[2 - \tfrac{55}{11}\cdot n\big]\cdot 33 \\ &= \underbrace{\big[-1+3n\big]}_{A_n}\cdot 55 + \underbrace{\big[2-5n\big]}_{B_n}\cdot 33\,. \end{aligned}$$

Our second LBolt gives that

$$1 = [-4]\cdot 11 + 3\cdot 15\,.$$

Our 1-parameter family of $(11,15)$-Bézout-pairs is thus

$$1 = \underbrace{[-4+15k]}_{X_k}\cdot 11 + \underbrace{[3-11k]}_{Y_k}\cdot 15\,.$$

Rewriting, $1 = 11\,X_k + 15\,Y_k$. Substituting,

$$\begin{aligned} 1 &= \big[55A_n + 33B_n\big]\cdot X_k + 15\cdot Y_k \\ &= 55\cdot\underbrace{A_nX_k}_{P_{n,k}} + 33\cdot\underbrace{B_nX_k}_{Q_{n,k}} + 15\cdot\underbrace{Y_k}_{R_{n,k}}\,. \end{aligned}$$

An *incomplete* 2-parameter family $\mathbf{V}_{n,k} := \begin{bmatrix} P_{n,k} \\ Q_{n,k} \\ R_{n,k} \end{bmatrix}$ of Bézout-triples for $(55,33,15)$ can be cheerfully written as

†:
$$\begin{aligned} P_{n,k} &= [-1+3n]\cdot[-4+15k]\,, \\ Q_{n,k} &= [2-5n]\cdot[-4+15k] \quad \textit{and} \\ R_{n,k} &= [3-11k]\,. \end{aligned}$$

Plugging in $n=0$ and $k=0$ gives the above $\begin{bmatrix} 4 \\ -8 \\ 3 \end{bmatrix}$. ♦

Going further. While correct triples $\begin{bmatrix} 7 \\ -8 \\ -8 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ -3 \\ 3 \end{bmatrix}$ and $\begin{bmatrix} -2 \\ 2 \\ 3 \end{bmatrix}$. can be obtained from (†), we need *non-integer* values of n,k to get them; e.g $\begin{bmatrix} 7 \\ -8 \\ -8 \end{bmatrix} = \mathbf{V}_{\frac{30}{55},1}$. *Unpleasant...*

Using another method [*Smith normal form* of a matrix], one can derive

‡:
$$\mathbf{U}_{\alpha,\beta} := \begin{bmatrix} 1 \\ -3 \\ 3 \end{bmatrix} + \alpha\begin{bmatrix} -3 \\ 10 \\ -11 \end{bmatrix} + \beta\begin{bmatrix} 0 \\ -5 \\ 11 \end{bmatrix}$$

which parametrizes all Bézout-triples, as α,β range over all the integers. E.g $\mathbf{U}_{-2,-3} = \begin{bmatrix} 7 \\ -8 \\ -8 \end{bmatrix}$ and $\mathbf{U}_{1,1} = \begin{bmatrix} -2 \\ 2 \\ 3 \end{bmatrix}$. ♦

Q4: Mon. 30 Jan With $M := 22$ and $\mathbf{J} := [0\,..\,M)$, use *repeated-squaring* to compute $6^{128} \equiv_M 4 \in \mathbf{J}$. Since 133 equals $2^7 + 2^2 + 2^0$, power $6^{133} \equiv_M 18 \in \mathbf{J}$.

[*Hint:* Compute with symm. residues, and use periodicity.]

RS Soln: The period is tiny, so this is quick.

```
(repeated-squaring 6 133 22 :symmod t)

 /--------------------- Mod 22 ----\
  n:      2^n |     Accum |   6^[2^n]
---+----------+-----------+-------------
  0:        1 |         1 |         6 <<
  1:        2 |         6 |        -8
  2:        4 |         6 |        -2 <<
  3:        8 |        10 |         4
  4:       16 |        10 |        -6
  5:       32 |        10 |        -8
  6:       64 |        10 |        -2
  7:      128 |        10 |         4 <<
All:     done |        -4 |
 \--------------------- Mod 22 ----/

  So  6^{133}  is mod-22 congruent to the
product of the << marked values, which is -4.
```

The upshot: $6^{128} \equiv_M 4$. And $6^{133} \equiv_M -4 \equiv_M 18$.

But *Whoa!?* –why can't we use Euler-φ? Alas, alack, $6 \not\perp 22$; *did we remember to check this?*

Q5: Fri. 03 Feb Carmichael fnc $\boldsymbol{\lambda}(385 \cdot 29 \cdot 43) = 2^A \cdot 3^B \cdot 5^C \cdot 7^D \cdot 11^E$

where $A = \underset{\llcorner\cdot\cdot\cdot\lrcorner}{2}$, $B = \underset{\llcorner\cdot\cdot\cdot\lrcorner}{1}$, $C = \underset{\llcorner\cdot\cdot\cdot\lrcorner}{1}$, $D = \underset{\llcorner\cdot\cdot\cdot\lrcorner}{1}$, $E = \underset{\llcorner\cdot\cdot\cdot\lrcorner}{0}$.

Euler-φ just for Fun... Our $K := 385 \cdot 29 \cdot 43$ factors as $K = 5 \cdot 7 \cdot 11 \cdot 29 \cdot 43$. So $\Phi(K)$ is gp-isomorphic to product of cyclic groups,

$$*: \quad \mathbb{Y}_{2^2} \times \mathbb{Y}_{2\cdot 3} \times \mathbb{Y}_{2\cdot 5} \times \mathbb{Y}_{2^2\cdot 7} \times \mathbb{Y}_{2\cdot 3\cdot 7}.$$

So $\varphi(K) = 2^7 \cdot 3^2 \cdot 5^1 \cdot 7^2 = 282240$ is the product of the group-orders. [For reference, $K = 480095$.] ♦

Good Carma! The $(*)$ gps are cyclic, so the exponent of the product group is simply the LCM of the group-orders.

Hence $\boldsymbol{\lambda}(K) = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^0 = 420$. ♦

Nota Bene: Were K a multiple of 4, we would use that $\Phi(2^{N+2}) \overset{\text{gp}}{\cong} \mathbb{Y}_2 \times \mathbb{Y}_{2^N}$.

Q6: Mon. 20 Feb Over alphabet $\mathbf{G} = \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$, our UD code has length-spectrum $\vec{\ell} = (1, 2, 2, 2, 2, 3)$. Its Kraft-sum equals $\Sigma(\vec{\ell}) = 1 - \underbrace{5/27}_{\text{.....}} = \underbrace{22/27}_{\text{.....}}$.

Ordering our alphabet as $\mathtt{a} < \mathtt{b} < \mathtt{c}$, the proof from our previous class constructs the following specific prefix code with spectrum $\vec{\ell}$:

$\underbrace{\mathtt{a}}_{\text{....}}$ $\underbrace{\mathtt{ba}}_{\text{....}}$ $\underbrace{\mathtt{bb}}_{\text{....}}$ $\underbrace{\mathtt{bc}}_{\text{....}}$ $\underbrace{\mathtt{ca}}_{\text{....}}$ $\underbrace{\mathtt{cba}}_{\text{....}}$.

Kraftyness. With alphabet size $\Gamma = 3$, the Kraft-sum of $\vec{\ell}$ is

$$\Sigma(\vec{\ell}) \coloneqq \Sigma_\Gamma(\vec{\ell}) \coloneqq \sum_{j=1}^{R} 1/\Gamma^{\ell_j},$$

where $\vec{\ell} = (\ell_1, \ldots, \ell_R)$ is the code's length-spectrum.

The first five lengths consume mass $\overbrace{1}^{1/3}, \overbrace{2, 2, 2,}^{1/3} \overbrace{2}^{1/9}$. Out of the $\frac{2}{9} = \frac{6}{27}$ of mass remaining, $\frac{1}{27}$ is eaten by the length-3. So this spectrum *fails* to be Γ-complete by mass $\frac{6}{27} - \frac{1}{27} = 5/27$.

Whence the above prefix-code? In order *shortest*-to-*longest*, we assign the *leftmost* available path down the tree. ["Leftmost" is well-defined, since we ordered the alphabet.]

BTWay, we can increase the Kraft-sum by shortening code-word cba to cb, but the code is still not 3-complete [not Γ-complete, for $\Gamma = 3$]. Indeed, there is *no* 3-complete spectrum $\vec{\mathbf{s}} \preccurlyeq \vec{\ell}$ satisfying $\Sigma(\vec{\mathbf{s}}) \leq 1$.

POSTING: *Removing the $\preccurlyeq\vec{\ell}$ restriction, prove there is no six word, 3-complete UD-code over $\mathbf{G} = \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$.* ♦

Home-U due, 11:30AM. Wed. 22 Feb ... slid under my office door, LIT402. *After* having successfully handed-in your Home-U, *email me* that you have done so, and include your Team-U number in the message.

Have printed-out Problem sheet, and made that the *first page* of youw write-up. Number the pages (probably by hand) 1/47 [that is the Problem sheet], 2/47 .... 47/47. Handwrite-in the blanks on the problem sheet, the requested answers.

Put name/ordinals/Team-number where requested, and sign the Honor Code.

Class-U. Wed. 22 Feb

In-class closed-book Open-Brain exam. Please bring lined-paper for computation. You may also want to bring colored pens/pencils for diagrams.

Q7: Fri. 24 Feb *Am I in class today?*

circle (one) *"Yes!"* *"Of course!"*

"I wouldn't miss it for the world!"

Q8: Fri. 10 Mar Congruences $z \equiv_{18} 5$, and $z \equiv_5 17$, fuse into $z \equiv_{90} T$, where $T =$ 77 $\in [0\,..\,90)$.

[Note: $\mathrm{LCM}(18,5) = 90$].

Nuclear fusion. Since $18 \perp 5$, we *could* use CRT.

```
% (fuse-many-mtars '(18 5) '(5 17))

  Starting fusion over ring "InTeGeRs".
  Our goal is to solve the following system of congruences:

  C1:  x ==   5            (mod  18 )
  C2:  x ==  17            (mod   5 )

  Here is a solution:

/-----------------------------------------------------\
With A:=18 and B:=5, is there an x with
  x =A=      5 and |  YES, since  D := Gcd(A,B) = 1  divides  5-17 =: F.
  x =B=     17 ?   |  Ratio is  R := F/D = -12.
  -----------------'
LBolt gives 2A + (-7)B =  D.  Multiplying by R produces
            (-24)A - (-84)B =  F  =  5 - 17.

  Thus  x + (-24)A  =  5.  So  x := 437  solves both congruences.
  Reducing this modulo  L := Lcm(A,B)=90 gives

                x := [437  mod  L]  =  77.

Upshot: We can fuse the two (Modulus Target) pairs into a
single (M T):
    (18, 5) fuse (5, 17)  ->  (L, x) =note= (90, 77) .
\-----------------------------------------------------/
```

Q9: Mon. 20 Mar Base-2 (distribution-)entropy of $\vec{v} := (\frac{1}{2}, \frac{1}{8}, \frac{1}{8}, \frac{1}{4})$ is $\mathcal{H}(\vec{v}) = \sum_p p \cdot \mathscr{L}(\frac{1}{p}) = \frac{1}{2} + \frac{3}{8} + \frac{3}{8} + \frac{2}{4} = \frac{14}{8} = 7/4$, .

Soln. ... *where*, $\mathscr{L}() := \log_2()$, ♦

The due-date for this year's *Robert Long Essay Competition (RLEC)* is Thurs., 30 Mar., with a PDF emailed to Prof. K. **True!** **Yes!**

QA: Fri. 24 Mar Legendre symbol $\left(\frac{47}{53}\right)$ is +1 −1 0.

Soln. *Fastest* –two lines– is Jacobi-LBolt:

```
% (setq   A 47   P 53)

% (jac A P  :symmod true)

                                                    Reason to negate J_n:
    n: Jn * (      T_n ==    TAU_n //       B_n) |     t_n | Xn | SIGN TWO QDRC
   --+-----------------------------------------+---------+----+--------------
    0:  1 * (       47 ==       -6 //        53) |       3 |  1 |      Two
    1: -1 * (       53 ==       -1 //         3) |       1 |    | Sign
    2:  1 * (        3 ==        0 //         1)  <-  This product equals 1.
```

Recall the nomenclature:

```
 Let Jn:=J_n, Tn=T_n, tn=t_n, TAUn:=TAU_n, etc..
 Note (0 // 1) = 1.  For D>1 odd, (0 // D) = 0.

>>  Product  Jn * (Tn // Bn)  will be preserved, as n=0,1,2,... .  <<

 We reduce  Tn == TAUn, mod Bn.  Here are actions that might negate Jn:
Each action is named in [Brackets].

 [Sign] If TAUn < 0 then change sign by replacing  TAUn  by  -TAUn.
      So if Bn is 4NEG then negate Jn.

 [Two] Factor  TAUn = tn * [2 ^ Xn], with tn posodd & natnum exponent Xn.
      If Xn odd  /and/  Bn =8= +-3, then negate Jn.

[QdRc] Quadratic Reciprocity.  Exchange tn with Bn to define the next row.
         (T_{n+1} // B_{n+1}) := (Bn // tn) * +-1.
      The "+-1" is -1  IFF  both tn and Bn were 4Neg.
```

Alt Soln. Also reasonable is repeated-squaring:

```
% (setq  H (/ (- P 1) 2)) => 26

% (repeated-squaring A H P)

    /--------------------- Mod 53 ----\
     n:      2^n |     Accum |  47^[2^n]
    ---+----------+-----------+-------------
     0:        1 |         1 |        47
     1:        2 |         1 |       -17 <<
     2:        4 |       -17 |        24
     3:        8 |       -17 |        -7 <<
     4:       16 |        13 |        -4 <<
    All:     done |         1 |
     \--------------------- Mod 53 ----/

     So  47^{26}  is mod-53 congruent to the
    product of the << marked values, which is 1.
```

Connected to (V2). Coincidentally, $53 \equiv_8 5$, so question (V2 γ) allows us to compute a sqroot of 47.

```
% (setq  ExponR (/ (+ P 3) 8))    => 7

% (repeated-squaring A ExponR P)

    /--------------------- Mod 53 ----\
     n:      2^n |     Accum |  47^[2^n]
    ---+----------+-----------+-------------
     0:        1 |         1 |        47 <<
     1:        2 |        -6 |       -17 <<
     2:        4 |        -4 |        24 <<
    All:     done |        10 |
     \--------------------- Mod 53 ----/

     So  47^{7}  is mod-53 congruent to the
   product of the << marked values, which is 10.

;; Checking...
% (mod 100 53)     => 47
```

QB: Fri. 14 Apr $\exists$*Math Festival* this **Sunday, ~~16~~Apr,** 10AM–1PM, in the *Rion Ballroom* of Reitz Union, open to all.

Circle: **True!** **Yes!** *What's* "Math"?

End of semester; looking forward to our Games Party!